Hopf–Galois Structures on Galois Extensions of Fields of Squarefree Degree

Submitted by Ali Abdulqader Bilal Alabdali to the University of Exeter

as a thesis for the degree of

Doctor of Philosophy in Mathematics

in May 2018

I certify that all material in this thesis which is not my own work has been identified and that no material has previously been submitted and approved for the award of a degree by this or any other university.

Signature: .....

Abstract

Hopf−Galois extensions were introduced by Chase and Sweedler [CS69] in 1969, motivated by the problem of formulating an analogue of Galois theory for inseparable extensions. Their approach shed a new light on separable extensions. Later in 1987, the concept of Hopf−Galois theory was further developed by Greither and Pareigis [GP87]. So, as a problem in the theory of groups, they explained the problem of finding all Hopf−Galois structures on a finite separable extension of fields. After that, many results on Hopf−Galois structures were obtained by N. Byott, T. Crespo, S. Carnahan, L. Childs, and T. Kohl.

In this thesis, we consider Hopf−Galois structures on Galois extensions of squarefree degree n. We first determine the number of isomorphism classes of groups G of order n whose centre and commutator subgroup have given orders, and we describe $\mathrm{Aut}(G)$ for each such G. By investigating regular cyclic subgroups in $\mathrm{Hol}(G)$, we enumerate the Hopf−Galois structures of type G on a cyclic extension of fields L/K of degree n. We then determine the total number of Hopf−Galois structures on L/K. Finally, we examine Hopf−Galois structures on a Galois extension L/K with arbitrary Galois group Γ of order n, and give a formula for the number of Hopf−Galois structures on L/K of a given type G.

Acknowledgements

In Iraq, I owe to my thanks and appreciation to the Higher Committee for Education Development in Iraq. Thank you for giving me the opportunity to continue my research. I am grateful for the financial support that enabled my doctoral study.
I also would like to express my deep thanks to the University of Mosul, College of Education for Pure Sciences, and Department of Mathematics and appreciate their supporting.

I am sincerely indebted to my supervisor Professor Nigel Byott for his continuous encouragement, motivation, patience, kindness, and immense knowledge, which enabled me to undertake my PhD study and related research. His guidance helped me in the research and writing the thesis.
I would like to express my sincere gratitude to the University of Exeter, College of Engineering, Mathematics, and Physical Sciences, and particularly Department of Mathematics for supporting and holding the seminars. I also would like to thank my PhD co-supervisor Professor Mohamed Saïdi for continuously supporting my progress.

At home, I am deeply thankful to all my family members, in particular my parents, my wife and my daughter for their love and generous sacrifices, and strongly supporting my endeavours that they provided me throughout my entire life and particularly during the past four years of completing the PhD degree.

Last but not least, I am grateful to all my friends for their enthusiasm, support and kindness, which served as a continual reminder of my interest in academic study.

Thus with all what have been saying above, I had the chance to complete this thesis.

Contents

Chapter 1

Introduction

1.1 Overview

In the late 1960s, Hopf−Galois theory was introduced in [CS69] by Chase and Sweedler. The motivation of their approach was a hope to generate a new version of Galois theory for inseparable field extensions. However, their project provides a significant viewpoint for separable extensions covered by the classical theory. After that, in 1987, Greither and Pareigis in [GP87] further investigated the idea of Hopf−Galois extension in separable field extensions. They showed the possibility of finding all Hopf−Galois structures on a separable extension L/K in terms of the theory of groups. Furthermore, they explained that L may admit many $H-$Galois structures for a number of different $K-$Hopf algebras H. As indicated in [CC07], it also emerged that different Hopf−Galois structures can arise because the Hopf algebra H itself could have different actions on L. So there are many terms related to Hopf−Galois extension, which is important to describe the Hopf−Galois structures on separable field extensions.

The aim of this thesis is to study the Hopf−Galois structures on a cyclic extension of fields of squarefree degree, or more generally, an arbitrary Galois extension of fields of squarefree degree. The extensions may admit many Hopf−Galois structures. The concept of Hopf algebras and the idea of Hopf−Galois structure on a finite separable

field extension play an essential role in this work. Thus we seek to enumerate and describe all Hopf−Galois structures which are admitted by a field extension. So we first review, analyze, and compare the previous work of some researchers.

Let L/K be a field extension of finite degree, and let H be a cocommutative $K-$Hopf algebra acting on L . We write $\Delta : H \longrightarrow H \otimes_K H$ and $\epsilon : H \longrightarrow K$ for the comultiplication and counit maps on H, and use Sweedler's notation $\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$. We will say that the action of H on L makes L into an $H-$module algebra if $h \cdot (xy) = \sum_{(h)}(h_{(1)} \cdot x) \otimes (h_{(2)} \cdot y)$ and $h \cdot k = \epsilon(h)k$ for all $h \in H$, all x, $y \in L$ and all $k \in K$. A Hopf−Galois structure on L consists of a Hopf algebra H acting on L so that L is an $H-$module algebra and the $K-$linear map $\theta : L \otimes_K L \longrightarrow \mathrm{Hom}_K(H, L)$ is bijective, where $\theta(x \otimes y)(h) = x(h \cdot y)$ for x, $y \in L$ and $h \in H$.

Let L/K be a finite Galois extension of fields with Galois group Γ. Then the group algebra $K[\Gamma]$ is a $K-$Hopf algebra, and its action on L endows L/K with a Hopf−Galois structure. In general, this is one among many possible Hopf−Galois structures on L/K. When L/K is separable, Greither and Pareigis [GP87] used descent theory to show how all Hopf−Galois structures on L/K could be described in group-theoretic terms. In the case that L/K is a Galois extension with group $\Gamma = \mathrm{Gal}(L/K)$, their key result is that the Hopf−Galois structures correspond bijectively to regular subgroups G of the group $\mathrm{Perm}(\Gamma)$ such that the left translations by Γ normalize the regular subgroups G. Although the two groups Γ and G need not be generally isomorphic, they should have the same order (i.e. $|\Gamma| = |G|$). We define the type of a Hopf−Galois structure to be the isomorphism type of G. Finding all Hopf−Galois structures in any particular case then becomes a combinatorial question in group theory. Recall that a group G acting on a set X is regular if the action is transitive on X and the stabiliser of any point is trivial.

The direct determination of all regular subgroups in $\mathrm{Perm}(\Gamma)$ normalised by $\lambda(\Gamma)$ is

often difficult as the group $\mathrm{Perm}(\Gamma)$ is large. Here, $\lambda : \Gamma \longrightarrow \mathrm{Perm}(\Gamma)$ is the left translation. However, the condition that $\lambda(\Gamma)$ normalises G means that Γ is contained in the holomorph $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ of G, where the latter group is viewed as a subgroup of $\mathrm{Perm}(\Gamma)$ and is usually much smaller than $\mathrm{Perm}(\Gamma)$. We may then view Γ as acting on G, and this action is again regular. If the isomorphism types of groups G^* of order $|\Gamma|$ admit a manageable classification, the Hopf−Galois structures on L/K can be determined by considering each G^* in turn and finding the regular subgroups Γ^* of $\mathrm{Hol}(G^*)$ which are isomorphic to Γ. This leads to the following result, cf. [Byo96, Cor. to Prop. 1] or [Chi00, §7]:

Lemma 1.1.1. Let L/K be a finite Galois extension of fields with Galois group Γ and, for any group G with $|G| = |\Gamma|$, let $e'(G, \Gamma)$ be the number of regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ. Then the number $e(G, \Gamma)$ of Hopf−Galois structures on L/K of type G is given by

$$e(G, \Gamma) = \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|}\, e'(G, \Gamma).$$

Moreover, the total number of Hopf−Galois structures on L/K is given by $\sum_G e(G, \Gamma)$, where the sum is over all isomorphism types G of groups of order $|\Gamma|$.

There is a substantial literature on Hopf−Galois structures on various classes of field extension. We briefly mention a few of the results.

The work of [Koh98] shows that if p is an odd prime, a cyclic extension of degree p^n admits p^{n-1} Hopf−Galois structures of cyclic type, whereas in [Chi05], an elementary abelian extension of degree p^n admits more than $p^{(n(n-1)-1)}(p-1)$ Hopf−Galois structures of elementary abelian type such that $p > n$. In [Byo04b], it is shown that if p and q are distinct primes with $p \equiv 1 \pmod{q}$ then a cyclic (respectively nonabelian) extension of degree pq has in total $2q-1$ (respectively $2+p(2q-3)$) Hopf−Galois structures. Whereas in [BC12], it is shown that most abelian extensions, except those of degree p or p^2 for p prime, admit Hopf−Galois structures of nonabelian type. More generally, the work of [Koh13] considers Galois field extensions L/K with $\Gamma = \mathrm{Gal}(L/K)$

of order mp such that p is a prime and $m < p$, and states a strategy for enumerating the regular subgroups of Perm(Γ) normalized by left representation of Γ, which are in bijection with the Hopf−Galois structures on L/K with Γ. Kohl proved that every regular subgroup is contained in the normalizer in Perm(Γ) of the $p-$Sylow subgroup of the left representation of Γ, and gave a number of examples, including the cases of groups whose order pq and $p(p-1)$ in [Byo04b] and [Chi03] respectively. In [Byo04a], it is shown that when Γ is a nonabelian simple group, the only Hopf−Galois structures are of type Γ; there are only two such Hopf−Galois structures, as shown in [CC99]. A Galois extension whose group $\Gamma = S_n$ is a symmetric group admits many Hopf−Galois structures of both type S_n and $A_n \times C_2$. If we compare the work in [Byo04b] and [Byo15], it is clear as mentioned in [Byo04b] above that either one of the groups Γ, G may be abelian while the other is nonabelian and, indeed, not nilpotent. The work in [Byo15] shows that if a Galois extension with group Γ admits a Hopf−Galois structure of nilpotent type then Γ is soluble, and that if Γ is abelian then G is soluble.

[Koh13, Koh16] has considered Galois extensions where the Galois group has a unique subgroup of some prime order p, in particular determining all Hopf-Galois structures on any Galois extension of degree $p_1p_2p_3$, where p_1, p_2, p_3 are distinct odd primes satisfying certain congruence conditions. Recently, Crespo, Rio and Vela [CRV16] have investigated those Hopf-Galois structures on an extension L/K which arise by combining Hopf-Galois structures on L/F and on F/K for some intermediate field F.

We now describe the contents of this thesis.

Chapter 2 contains background information about algebras and Hopf algebras, regular embeddings, the Greither−Pareigis Theorem, Byott's Translation, and Kohl's formulation.

Chapter 3 contains investigation about the groups G of squarefree order n. We have obtained the number of isomorphism classes with central and commutator subgroups of given order. Moreover, we determine the order of $\mathrm{Aut}(G)$. Then we find some elements which generate cyclic subgroup of $\mathrm{Hol}(G)$.

In Chapter 4, we examine Hopf−Galois structures on a cyclic field extension L/K of squarefree degree n. We prove two results counting Hopf−Galois structures. We explain that if L/K is a cyclic extension of fields of squarefree degree n and G is any group of order n, then there is a nice formula for counting the number of Hopf−Galois structures of type G on L/K. Also, we show another formula enumerating the total number of Hopf−Galois structures on a cyclic extension of fields of squarefree degree n. Finally, we give some examples such as cyclic Hopf−Galois structures, dihedral Hopf−Galois structures, and we consider groups whose order is the product of two, three or four distinct primes. Thus we show that how some results from the literature in Chapter 2 can be obtained as special cases of our results.

The material in Chapter 3 and Chapter 4 has been published in the paper [AB18] in the Journal of Algebra in January 2018.

In Chapter 5, we extend the methods of Chapter 4 to investigate Hopf−Galois structures on an arbitrary Galois field extension L/K of squarefree degree n. Then we count the number of Hopf−Galois structures of a given type. After that, we give some examples of special cases where either one of G or Γ is a cyclic or dihedral group, and find the number of Hopf−Galois structures of these types.

On the one hand, these results may have applications to Galois module theory in number theory. On the other hand, particularly in mathematical physics, they are related to the problem of classifying skew braces of squarefree order, and therefore to solutions

of the quantum Yang−Baxter equation.

Guarnieri and Vendramin in [GV17] defined (left) skew brace as a triple $(A, *, \circ)$ which consists of a set A together with two operations $*$ and $\circ$ such that $(A, *)$ and $(A, \circ)$ are groups (neither necessarily abelian), and the two operations are related by the skew brace property:

$$a \circ (b * c) = (a \circ b)a^{-1} * (a \circ c) \text{ for every } a, b, c \in A,$$

where a^{-1} is the inverse of a with respect to the operation $*$.

In [Dri92] Drinfeld studied the problem of set−theoretical solutions of the Yang−Baxter equation. Let X be a set and $r : X \times X \longrightarrow X \times X$ by $r(x, y) \mapsto (f_x(y), g_y(x))$ where $f_x, g_x : X \longrightarrow X$ be a bijection such that:

$$(r \times id)(id \times r)(r \times id) = (id \times r)(r \times id)(id \times r).$$

Then the pair (X, r) is called set−theoretic solutions of the Yang−Baxter equation, and skew braces give rise to certain solutions of the Yang−Baxter equation. On the other hand, if $(A, *, \circ)$ is a skew brace, then we may view $(A, \circ)$ as a regular subgroup of $\mathrm{Hol}(A, *)$. Thus counting the number of skew braces (up to isomorphism) with $(A, \circ)$ isomorphic to Γ and $(A, *)$ isomorphic to G is closely related to counting the number of Hopf-Galois structures of type G on a Galois extension with Galois group isomorphic to Γ.

Chapter 2

Background

In this chapter, we firstly introduce the basic concepts and algebraic and arithmetic results which we will need in the next chapters. We then present Hopf algebras and the notion of a Hopf−Galois structure on a finite separable extension of fields, along with theorems which help us to count and describe all of the Hopf−Galois structures admitted by a given extension. The following definitions and results will allow us to study the concept of Hopf−Galois structures. Our main references in this chapter are the papers by Byott [Byo96], [Byo15], Kohl [Koh13], [Koh16] and the book by Childs [Chi00].

2.1 Hopf−Galois structure

Certain extensions of commutative rings define the notion of a Hopf−Galois structure. This work will be concerned with the study of Hopf−Galois structures on finite separable field extensions.

2.1.1 Algebra and Hopf algebra

Definition 2.1.1. Let R be a commutative ring with unity. An $R-$module H with the multiplication map $\mu : H \otimes_R H \longrightarrow H$ and a unit map $\iota : R \longrightarrow H$ is called an $R-$algebra if the following diagrams commute:

- Associativity:

$$\begin{array}{ccc} H \otimes_R H \otimes_R H & \xrightarrow{\mu\otimes 1} & H \otimes_R H \\ {\scriptstyle 1\otimes\mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ H \otimes_R H & \xrightarrow[\mu]{} & H \end{array}$$

- Unitary property:

$$\begin{array}{ccc} H \otimes_R R & \xrightarrow{1\otimes\iota} & H \otimes_R H \\ \| & & \downarrow{\scriptstyle \mu} \\ H \otimes_R R & \xrightarrow[scalar\ \ mult.]{} & H \end{array}$$

and

$$\begin{array}{ccc} R \otimes_R H & \xrightarrow{\iota\otimes 1} & H \otimes_R H \\ \| & & \downarrow{\scriptstyle \mu} \\ R \otimes_R H & \xrightarrow[scalar\ \ mult.]{} & H \end{array}$$

Definition 2.1.2. Let R be a commutative ring with unity. An $R-$algebra H with the comultiplication map $\Delta : H \longrightarrow H \otimes_R H$ and counit map $\epsilon : H \longrightarrow R$ is called an $R-$bialgebra, where Δ and ϵ are $R-$algebra homomorphisms and the multiplication in $H \otimes H$ has the form $(h \otimes j)(h^{'} \otimes j^{'}) = hh^{'} \otimes jj^{'}$. The $R-$algebra homomorphisms Δ and ϵ satisfy the following properties:

- Coassociativity:

$$\begin{array}{ccc} H & \xrightarrow{\Delta} & H \otimes_R H \\ {\scriptstyle \Delta}\downarrow & & \downarrow{\scriptstyle \Delta\otimes 1} \\ H \otimes_R H & \xrightarrow[1\otimes\Delta]{} & H \otimes_R H \otimes_R H \end{array}$$

- Counitary property:

$$\begin{array}{ccc} H & \xrightarrow{\Delta} & H \otimes_R H \\ \| & & \downarrow{\scriptstyle 1\otimes\epsilon} \\ H & \xleftarrow[\mu]{} & H \otimes_R R \end{array}$$

and

$$\begin{array}{ccc} H & \xrightarrow{\Delta} & H \otimes_R H \\ \| & & \downarrow{\scriptstyle \epsilon\otimes 1} \\ H & \xleftarrow[\mu]{} & R \otimes_R H \end{array}$$

Definition 2.1.3. An $R-$coalgebra is an $R-$module which possesses the counit and comultiplication maps.

Definition 2.1.4. The map $\tau : H \otimes_R H \longrightarrow H \otimes_R H$ is called the switch map if it satisfies $\tau(h_1 \otimes h_2) = h_2 \otimes h_1$.

Definition 2.1.5. Let R be a commutative ring with unity. An $R-$Hopf algebra is an $R-$bialgebra H with multiplication map $\mu : H \otimes H \longrightarrow H$, unit map $\iota : R \longrightarrow H$, comultiplication map $\Delta : H \longrightarrow H \otimes_R H$ and counit map $\epsilon : H \longrightarrow R$ for which there is an $R-$module homomorphism $\lambda : H \longrightarrow H$ (the antipode map) satisfying the following properties:

1. λ is an $R-$algebra antihomomorphism. That is, $\lambda(h_1h_2) = \lambda(h_2)\lambda(h_1)$.
2. λ is an $R-$coalgebra antihomomorphism. That is, $\Delta\lambda(h) = (\lambda \otimes \lambda)\tau\Delta(h)$.
3. λ satisfies the antipode property: $\mu(1 \otimes \lambda)\Delta = \iota\epsilon = \mu(\lambda \otimes 1)\Delta$.

Definition 2.1.6. An $R-$Hopf algebra H is said to be:

1. commutative if it is commutative as an $R-$algebra.
2. cocommutative if $\tau\Delta = \Delta$.
3. abelian if it satisfies both commutative and cocommutative conditions.

Definition 2.1.7. We adopt Sweedler's notation, as used in [CS69]. Let R be a commutative ring with unity and let H be an $R-$Hopf algebra. For $h \in H$, we define

$$\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)} \in H \otimes_R H.$$

Definition 2.1.8. Let R be a commutative ring with unity. Let S be an $R-$algebra which is also an $H-$module where H is an $R-$Hopf algebra. Then S is called an $H-$module algebra if we have

$$h(st) = \sum_{(h)} h_{(1)}(s)h_{(2)}(t),$$

and

$$h(1) = \epsilon(h)1 \text{ for all } h \in H \text{ and } s, t \in S.$$

Definition 2.1.9. An $R-$Hopf algebra which is finitely generated and projective as an $R-$module is called a finite $R-$Hopf algebra.

Definition 2.1.10. Let R be a commutative ring with unity. Let H be a finite $R-$Hopf algebra, and let $R \subseteq S$ be a commutative ring such that S is an $H-$module algebra. Then we say that S is an $H-$Galois extension. In other words, H gives a Hopf−Galois structure on the extension if the $R-$module homomorphism

$$j : S \otimes_R H \longrightarrow \mathrm{End}_R(S)$$

defined as

$$j(s \otimes h)(t) = sh(t) \text{ for } s, t \in S, h \in H$$

is an isomorphism.

Example 2.1.11. Let Γ be a group . The bialgebra $K[\Gamma]$, with antipode λ given by $\gamma \mapsto \gamma^{-1}$ for all $\gamma \in \Gamma$, is a Hopf algebra and it is a cocommutative Hopf algebra, since the comultiplication Δ is given by $\gamma \mapsto \gamma \otimes \gamma$.

Definition 2.1.12. Let L/K be a finite Galois extension of fields with $\Gamma = \mathrm{Gal}(L/K)$. The $K-$Hopf algebra $H = K[\Gamma]$ acts on L, so that L is an $H-$module algebra. Then the action on L makes L into a $H-$Galois extension and gives L a Hopf−Galois structure. Therefore, the Hopf−Galois structure on the extension produced by the Hopf algebra $K[\Gamma]$ is called the classical structure, whilst the other Hopf−Galois structures admitted by the extension are called nonclassical.

2.1.2 Regular embedding

Definition 2.1.13. Let $\mathrm{Perm}(X)$ be the group of permutations of a finite set X. A subgroup H of a group $\mathrm{Perm}(X)$ is said to be regular if it satisfies any two of the following properties which imply to satisfy the other:

1. $Stab_H(x) = \{h \in H | h(x) = x\}$ is the trivial group, for any $x \in X$;
2. H acts transitively on X;
3. $|H| = |X|$.

Thus $H \subset \mathrm{Perm}(X)$ is regular if and only if for some $x \in X$ (hence for all $x \in X$), the map from H to X by $h \mapsto h(x)$ is bijective.

Definition 2.1.14. Let G be a group and $\lambda(G) : G \longrightarrow \mathrm{Perm}(G)$. The holomorph of G, $\mathrm{Hol}(G)$, is the normaliser of $\lambda(G)$ in $\mathrm{Perm}(G)$, that means it is a subgroup of a group $\mathrm{Perm}(G)$:

$$\mathrm{Hol}(G) = \{\sigma \in \mathrm{Perm}(G) | \, \sigma \text{ normalises } \lambda(G)\}.$$

Definition 2.1.15. Let Γ be a group and let $\beta : \Gamma \longrightarrow \mathrm{Hol}(G)$. Then β is said to be regular embedding if:

1. β is a group homomorphism;
2. β is injective;
3. $im(\beta) = \beta(\Gamma)$ is a regular subgroup of permutations of G.

2.2 Greither−Pareigis Theorem

We are given a finite separable extension of fields L/K. By the theorem of Greither and Pareigis (Theorem 2.2.7 below), it is possible to see how many different Hopf−Galois structures are admitted by this extension. Also it provides a theoretical description of the Hopf algebras. This fundamental result means that the Hopf−Galois theory developed by Chase and Sweedler leads to interesting questions even for field extensions which are already Galois in the classical sense.

Theorem 2.2.1. Let X be a finite set and E a field. We can define $u_x : X \longrightarrow E$ by $u_x(y) = \delta_{x,y}$ for all $x, y \in X$, where $\delta_{x,y}$ is the Kronecker delta. Then $\{u_x : x \in X\}$ is an $E-$basis of the $E-$vector space $XE = \mathrm{Map}(X, E)$ and is a set of primitive pairwise orthogonal idempotents of XE. If H is a finite cocommutative $E-$Hopf algebra such that XE is an $H-$Hopf Galois extension of E, then H is a group ring EG for G some group of the same cardinality as X. As the action of G on X is defined by $\eta(u_x) = u_{\eta(x)}$ for all $x \in X$, $\eta \in G$, then G may be defined as a subgroup of $\mathrm{Perm}(X)$. Therefore, G is a regular subgroup of $\mathrm{Perm}(X)$. Conversely, if G is a regular subgroup of $\mathrm{Perm}(X)$, then XE is $EG-$Galois.

Proof. See [Chi00, 6.3]. □

Definition 2.2.2. Let Γ be a group and suppose Γ' is a subgroup of Γ. Let X be the left coset space Γ/Γ' of Γ' in Γ, so $X = \{\gamma\Gamma' | \gamma \in \Gamma\}$. We shall write $\overline{\gamma}$ for the coset $\gamma\Gamma'$. Then we can define the left translation map as

$$\lambda : \Gamma \longrightarrow \mathrm{Perm}(X)$$

by:

$$\lambda(\gamma)(\overline{\delta}) = \overline{\gamma\delta} \text{ for } \gamma \in \Gamma \text{ and } \overline{\delta} \in X.$$

Proposition 2.2.3. Let L/K be a finite separable extension of fields with Galois

closure E. Let $\Gamma = \mathrm{Gal}(E/K)$, $\Gamma' = \mathrm{Gal}(E/L)$ and $X = \Gamma/\Gamma'$. Then the map λ is one−to−one, in other words it is an embedding of Γ into $\mathrm{Perm}(X)$.

Proof. See [Chi00, 6.6]. □

Definition 2.2.4. Let $\gamma \in \Gamma$ and $\pi \in \mathrm{Perm}(X)$. A left action of Γ on $\mathrm{Perm}(X)$ is defined by a conjugation via the embedding $\lambda(\Gamma)$. So we set

$$^{\gamma}\pi = \lambda(\gamma)\pi\lambda(\gamma^{-1}).$$

In Proposition 2.2.3, if L/K is a Galois extension, then $\Gamma' = \{1\}$ and $X = \Gamma$.

Definition 2.2.5. It is easy to see that the right translation map can be defined as: if L/K is a Galois extension, then we have the right translation map as follows

$$\rho : \Gamma \longrightarrow \mathrm{Perm}(X)$$

by:

$$\rho(\gamma)(x) = x\gamma^{-1} \text{ for } \gamma \in \Gamma \text{ and } x \in X.$$

So this is an embedding of Γ into $\mathrm{Perm}(X)$.

Example 2.2.6. Let L/K be a Galois extension with group $\Gamma = \mathrm{Gal}(L/K)$. Then Γ is embedded as a regular subgroup inside $\mathrm{Perm}(\Gamma)$ in two ways:

$$\lambda : \Gamma \longrightarrow \mathrm{Perm}(\Gamma),$$

$\lambda(\sigma)(\tau) = \sigma\tau$, left translation, and

$$\rho : \Gamma \longrightarrow \mathrm{Perm}(\Gamma),$$

$\rho(\sigma)(\tau) = \tau\sigma^{-1}$, right translation:

$$(\rho(\sigma_1\sigma_2))(\tau) = \tau(\sigma_1\sigma_2)^{-1} = \tau\sigma_2^{-1}\sigma_1^{-1} = \rho(\sigma_1)(\tau\sigma_2^{-1}) = \rho(\sigma_1)\rho(\sigma_2)(\tau).$$

We claim, $\lambda(\Gamma) = \rho(\Gamma) \subset \mathrm{Perm}(\Gamma)$ if and only if Γ is abelian.

If Γ is abelian, then $\rho(\sigma) = \lambda(\sigma^{-1})$. Conversely, if $\rho(\sigma) = \lambda(\pi)$, then $\pi = \sigma^{-1}$ for some $\sigma, \pi \in \Gamma$, since $\rho(\sigma)e = \sigma^{-1} = \lambda(\sigma^{-1})e$. However, if $\sigma\tau \neq \tau\sigma$ for some $\sigma, \tau \in \Gamma$, then $\rho(\sigma) \neq \lambda(\sigma^{-1})$: for $\rho(\sigma)\tau = \tau\sigma^{-1} \neq \sigma^{-1}\tau = \lambda(\sigma^{-1})\tau$. So $\rho(\sigma) \notin \lambda(\Gamma)$.

Since $\lambda(\Gamma)$ normalizes itself and commutes with $\rho(\Gamma)$ in $\mathrm{Perm}(\Gamma)$, both $\lambda(\Gamma)$ and $\rho(\Gamma)$ are regular subgroups of $\mathrm{Perm}(\Gamma)$ normalized by $\lambda(\Gamma)$.

Theorem 2.2.7. (Greither−Pareigis) Let L/K be a finite separable extension of fields with Galois closure E. Let $\Gamma = \mathrm{Gal}(E/K)$, $\Gamma' = \mathrm{Gal}(E/L)$ and $X = \Gamma/\Gamma'$. Then there is a one−to−one correspondence between regular subgroups G of $\mathrm{Perm}(X)$ that are normalised by $\lambda(\Gamma)$ and Hopf−Galois structures on L/K. If G is a regular subgroup, then Γ acts on the group algebra $E[G]$ as the Galois group on E, and on the group elements by conjugation via $\lambda(\Gamma)$. The Hopf−Galois structure that corresponds to the regular subgroup G is given by the Hopf algebra as

$$H = E[G]^{\Gamma} = \{\pi \in E[G] \mid {}^{\gamma}\pi = \pi \text{ for all } \gamma \in \Gamma\}.$$

Then the Hopf algebra acts on the field extension L/K as follows: for $\left(\sum_{g\in G} s_g g\right) \in H$ where $s_g \in E$, we have

$$\left(\sum_{g\in G} s_g g\right) x = \sum_{g\in G} s_g(g^{-1}(\overline{1_\Gamma}))x.$$

Proof. See [Chi00, 6.8]. □

Proposition 2.2.8. Let L/K be a Galois extension with group Γ, and let $\rho : \Gamma \longrightarrow \mathrm{Perm}(\Gamma)$ be the right translation. Then $\rho(\Gamma)$ corresponds to the classical action of Γ on L.

Proof. See [Chi00, 6.10]. □

Corollary 2.2.9. Let L/K be a Galois extension with nonabelian group Γ, then L/K has a nonclassical Hopf−Galois structure, in other words, the structure that corresponds

to the regular subgroup $G = \lambda(\Gamma) \neq \rho(\Gamma)$.

Proof. See [Chi00, 6.11]. □

Definition 2.2.10. The type of the Hopf algebra will refer to the isomorphism class of the group G if H is a Hopf algebra presented by Theorem 2.2.7.

2.3 Byott's Translation

There is a difficulty in using the Greither−Pareigis theorem if we apply it directly to count the number of Hopf−Galois structures on a finite separable field extension L/K. The difficult problem starts when the order of the group Γ is more than 4, which means there are a large number of regular subgroups of $\mathrm{Perm}(\Gamma/\Gamma')$. Therefore, we need to seek which regular subgroups are normalised by Γ. However, the translation of [Byo96] is based on the observations of [GP87] and [Chi89] to overcome this problem. It facilitates easier calculations by reversing the relationship between the group Γ and the regular subgroups G.

Proposition 2.3.1. Let G be a finite group. The right translation map $\rho : G \longrightarrow \mathrm{Perm}(G)$ is a regular embedding of G into $\mathrm{Perm}(G)$ (see Definition 2.2.5) and we have:

$$\mathrm{Hol}(G) = \rho(G) \rtimes \mathrm{Aut}(G).$$

Proof. See [Chi00, 7.2]. □

Theorem 2.3.2. (Byott's Translation) Let $\Gamma' \subset \Gamma$ be finite groups, let $X = \Gamma/\Gamma'$ and let G be an abstract group of order $|X|$. Then there is a bijection between the following two sets:

$$\begin{aligned}\mathcal{G} = &\{\alpha : G \longrightarrow \mathrm{Perm}(X) | \alpha \text{ an injective homomorphism} \\ &\text{such that } \alpha(G) \text{ is regular}\}\end{aligned}$$

and

$$\mathcal{H} = \{\beta : \Gamma \longrightarrow \mathrm{Perm}(G) | \beta \text{ an injective homomorphism such that } \beta(\Gamma') = Stab_{\beta(\Gamma)}(1_G)\}.$$

Under this bijection, if α, $\alpha' \in \mathcal{G}$ correspond to β, $\beta' \in \mathcal{H}$ respectively, then:

- $\alpha(G) = \alpha'(G)$ if and only if $\beta(\Gamma)$ and $\beta'(\Gamma)$ are conjugate by an element of $\mathrm{Aut}(G)$.
- $\alpha(G)$ is normalised by $\lambda(\Gamma) \subset \mathrm{Perm}(X)$ if and only if $\beta(\Gamma)$ is contained in $\mathrm{Hol}(G)$, the normaliser of G in $\mathrm{Perm}(G)$.

Proof. Originally [Byo96, Proposition 1]. This formulation [Chi00, 7.3]. □

We can use Byott's theorem for counting Hopf−Galois structures on a finite separable extension of fields L/K as follows:

Corollary 2.3.3. Let L/K be a finite separable extension of fields with Galois closure E. Let $\Gamma = \mathrm{Gal}(E/K)$, $\Gamma' = \mathrm{Gal}(E/L)$. Let S be the set of isomorphism classes of groups G with $|G| = |\Gamma/\Gamma'|$. Then the number of Hopf−Galois structures of type G on L/K is given by

$$e(\Gamma, \Gamma', G) = \frac{|\mathrm{Aut}(\Gamma, \Gamma')|}{|\mathrm{Aut}(G)|} e'(\Gamma, \Gamma', G),$$

where $e'(\Gamma, \Gamma', G)$ is the number of subgroups Γ^* of $\mathrm{Hol}(G)$ such that there exists an isomorphism from Γ^* to Γ taking the stabiliser in Γ^* of 1_G to Γ', for each $[G] \in S$, and

$$\mathrm{Aut}(\Gamma, \Gamma') = \{\sigma \in \mathrm{Aut}(\Gamma) \,|\, \sigma(\Gamma') = \Gamma'\}.$$

The total number of Hopf−Galois structures admitted by the extension is given by

$$\sum_{[G] \in S} e(\Gamma, \Gamma', G).$$

Proof. See [Chi00, 7.6]. □

We will only apply this formula of Corollary 2.3.3 when the extension L/K is normal i.e. it is a Galois extension, when it reduces to the following formula such that $\Gamma' = \{1_\Gamma\}$. Then $X = \Gamma$, $\mathrm{Aut}(\Gamma, \Gamma') = \mathrm{Aut}(\Gamma)$ and we write the quantities $e(\Gamma, \Gamma', G)$ and $e'(\Gamma, \Gamma', G)$ as $e(\Gamma, G)$ and $e'(\Gamma, G)$ respectively.

$$e(\Gamma, G) = \frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|}\, e'(\Gamma, G),$$

where $e'(\Gamma, G)$ is the number of regular subgroups of $\mathrm{Hol}(G)$ which are isomorphic to Γ. Therefore, the total number of Hopf−Galois structures admitted by the extension is given by

$$\sum_{[G]\in S} e(\Gamma, G).$$

2.4 Kohl's formulation

Let L/K be a finite Galois extension with a Galois group $\Gamma = \mathrm{Gal}(L/K)$.

The inspiration of Kohl's ideas and previous works relates to the subject of Hopf−Galois theory for Galois field extensions. In particular, in [Koh13] Kohl considered the cases that $|\Gamma| = mp$ for p prime such that $p > m$, whilst in [Koh16] he tried to extend the previous results in groups of order mp with $\gcd(p, m) = 1$ without making $p > m$. But he still needed some assumptions on p and m, otherwise it will be a hugely general result. Kohl uses the general theory which includes the basic definitions and essential examples that were developed in [CS69] and [GP87] and applied for separable extensions.

In [Koh13], Kohl considered groups Γ of order mp with $p > m$ because that guarantees there is a unique Sylow p−subgroup. Due to the Schur−Zassenhaus lemma, Γ could be assumed as PQ where P and Q are two subgroups of Γ such that $|P| = p$ and $|Q| = m$, in other words there is $P \longrightarrow \Gamma \longrightarrow Q$ as an exact sequence where $\Gamma = P \rtimes_\tau Q$ and $\tau : Q \longrightarrow \mathrm{Aut}(P)$. So to get a unique Sylow p−subgroup with order p, it is enough to impose the condition $p > m$. Since the left regular representation $\lambda : \Gamma \longrightarrow \mathrm{Perm}(\Gamma) = T$, then $\mathcal{P} = \langle \pi \rangle = \langle \pi_1 \pi_2 \cdots \pi_m \rangle = P[\lambda(\Gamma)]$ has been defined as the Sylow p−subgroup

of $\lambda(\Gamma)$ and $\mathcal{Q}$ to be the complementary subgroup to $\mathcal{P}$ in $\lambda(\Gamma)$. It is clear that Kohl had worked out a new method for counting the regular subgroups by looking for them inside $\mathrm{Norm}_T(\mathcal{P})$, the normaliser in T of $\mathcal{P}$.

Definition 2.4.1. Let M be a group of the same order as Γ and $[M]$ the isomorphism class of M. So we can define

$$R(\Gamma, [M]) = \{G \leq T = \mathrm{Perm}(\Gamma) \mid G \text{ regular}, G \cong M, \lambda(\Gamma) \leq \mathrm{Norm}_T(G)\}$$

and

$$R(\Gamma) = \bigcup_{[M]} R(\Gamma, [M]).$$

Theorem 2.4.2. Let Γ have order mp where $\gcd(p, m) = 1$. If $G \in R(\Gamma)$ then G is a subgroup of $\mathrm{Norm}_T(\mathcal{P})$ under the assumptions that all groups of order mp have a unique Sylow $p-$subgroup and $p \nmid |\mathrm{Aut}(Q)|$ for any group Q of order m.

Proof. See [Koh16, Theorem 1.3]. □

Definition 2.4.3. Let A be a finite set and G a subgroup of a group $\mathrm{Perm}(A)$. Then G is said to be a semiregular if each element of G except the identity acts on A without fixed points.

The next theorem will guarantee that $P(G) \leq \mathcal{S} \leq \mathrm{Norm}_T(\mathcal{P})$ for all $G \in R(\Gamma)$ where $\mathcal{S} = \langle \pi_1, \pi_2, \cdots, \pi_m \rangle$ and π_i are disjoint $p-$cycles, $i = 1, \ldots, m$, and $P(G)$ is a Sylow $p-$subgroup of G and is cyclic of order p, therefore $P(G) = \langle \theta \rangle = \langle \theta_1 \theta_2 \cdots \theta_m \rangle$ where θ_i are also disjoint $p-$cycles, $i = 1, \ldots, m$.

Theorem 2.4.4. $P(G)$ is a semiregular subgroup of $\mathcal{S}$ if G is a regular subgroup of T normalised by $\lambda(\Gamma)$ and $P(G)$ is its Sylow $p-$subgroup. That is, $P(G) = \langle \pi_1^{a_1} \pi_2^{a_2} \cdots \pi_m^{a_m} \rangle$ where $a_i \in U_p = \mathbb{F}_p^\times$ for $i = 1, \ldots, m$.

Proof. See [Koh16, Theorem 1.6]. □

Theorem 2.4.5. Let G be a regular subgroup of a group $T = \mathrm{Perm}(\Gamma)$ normalised by left representation of Γ, $\lambda(\Gamma) = \mathcal{PQ}$. Then G is a subgroup of $\mathrm{Norm}_T(\mathcal{P})$.

Proof. See [Koh13, Theorem 3.5]. □

Kohl studies in [Koh13] and [Koh16] the groups of order $p_1p_2p_3$ where p_1, p_2, p_3 are primes such that $p_1 < p_2 < p_3$. So in [Koh13], he considers groups of order $2pq$ where p and q are odd primes such that $p = 2q + 1$. Therefore, there are six isomorphism types of groups of order $2qp$ as follow $C_{mp}, C_p \times D_q, C_q \times D_p, D_{pq}, F \times C_2,$ and $\mathrm{Hol}(C_p)$. Then he shows in [Koh13, Theorem 5.1] the number of Hopf−Galois structures of type (the groups above) on a Galois extension L/K with Galois grooup Γ.

In [Koh16], Kohl considers the groups of order mp with the condition $\gcd(p, m) = 1$ instead of the assumption that $p > m$ for p prime. Kohl assumes p and m are such that any group of order mp has a unique Sylow p−subgroup. He shows that if the order of the group Γ is $p_1p_2p_3$ where $p_1 < p_2 < p_3$ are primes, then $\Gamma = \mathcal{P}\mathcal{Q}$ where $\mathcal{P}$ is cyclic of order p_3 normalised by $\mathcal{Q}$ and $\mathcal{Q}$ is a direct or semidirect product of cyclic groups of order p_1p_2. Therefore, $\Gamma \cong C_{p_3} \rtimes_{\mathcal{G}} (C_{p_2} \rtimes_{\mathcal{F}} C_{p_1})$ where $\mathcal{F} : C_{p_1} \longrightarrow \mathrm{Aut}(C_{p_2})$ and $\mathcal{G} : C_{p_2} \rtimes_{\mathcal{F}} C_{p_1} \longrightarrow \mathrm{Aut}(C_{p_3})$. There are at most two groups $\mathcal{Q}$ of order p_1p_2 up to isomorphism, and which one arises depends on whether or not $\mathcal{F}$ is trivial. The isomorphism type of Γ depends on the isomorphism type of $\mathcal{Q}$ and on $\mathcal{G}$. To show how many possible groups Γ there are, we must know whether C_{p_2} and/or C_{p_1} act nontrivially on C_{p_3}. The congruence conditions on the primes p_1, p_2, p_3 are based on the possibilities for $\mathcal{F}$ and $\mathcal{G}$. In particular, whether $p_1 \mid (p_2 - 1)$ and/or $p_1 \mid (p_3 - 1)$ and/or $p_2 \mid (p_3 - 1)$.

Proposition 2.4.6. Let p_1, p_2, p_3 are distinct odd primes, where $p_1 < p_2 < p_3$ and $p_1 \mid (p_2 - 1)$, $p_1 \mid (p_3 - 1)$ but $p_2 \nmid (p_3 - 1)$. Then there are $p_1 + 2$ groups of order $p_1p_2p_3$ as follows: $C_{p_1p_2p_3}$, $C_{p_2} \times (C_{p_3} \rtimes C_{p_1})$, $C_{p_3} \times (C_{p_2} \rtimes C_{p_1})$, and $C_{p_2p_3} \rtimes_i C_{p_1}$, where $i = 1, \ldots, p_1 - 1$.

Proof. See [Koh16, Propsition 2.1]. □

Then Kohl in [Koh16, Theorem 2.4] shows the number of Hopf−Galois structures for

the $p_1 + 2$ different isomorphism classes of groups of order $p_1p_2p_3$ given in 2.4.6.

Chapter 3

Groups of Squarefree Order

In this chapter, we work with the groups G of squarefree order n. We investigate the number of isomorphism classes of these groups, which is important proposition in the proof of one of the main theorems in Chapter 4. Also, we find the order of $\mathrm{Aut}(G)$. Then we produce some element which generate cyclic subgroups of $\mathrm{Hol}(G)$.

3.1 Preliminaries on groups of squarefree order

We will call a finite group a $C-$group if all its Sylow subgroups are cyclic. In particular, any group of squarefree order is a $C-$group. All $C-$groups are metabelian, so $C-$groups can in principle be classified [Rob96, 10.1.10]. This classification is given in a rather explicit form in a paper of Murty and Murty [MM84], who investigated the asymptotic behaviour of the number of $C-$groups of order up to a given bound. We state their classification result, in the special case of groups of squarefree order, as Lemma 3.1.2 below. In addition to that, Hölder [Höl95] showed that the number of isomorphism types of groups of squarefree order n is given by

$$\sum_{de=n} \prod_{p|d} \left(\frac{p^{v(p,e)} - 1}{p - 1} \right), \tag{3.1}$$

where the sum is over ordered pairs (d, e) of positive integers such that $de = n$, the product is over primes p dividing d, and $v(p, e)$ is the number of distinct prime factors q of e with $q \equiv 1 \pmod{p}$. It is clear that, as n varies over all squarefree integers, the expression (3.1) can become arbitrarily large.

Notation 3.1.1. For an integer $N \geq 1$, we denote by $\mathbb{Z}_N$ the ring $\mathbb{Z}/N\mathbb{Z}$ of integers modulo N, and by $U(N)$ the group of units in $\mathbb{Z}_N$. We write $\mathrm{ord}_N(a)$ for the order of an element $a \in U(N)$. Abusing notation, we will often use the same symbol for an element of $\mathbb{Z}$ and its class in $\mathbb{Z}_N$. We write 1_G for the identity element of a group G.

Lemma 3.1.2. Let n be squarefree. Then any group of order n has the form

$$G(d, e, k) = \langle \sigma, \tau \colon \sigma^e = \tau^d = 1_G, \tau\sigma\tau^{-1} = \sigma^k \rangle$$

where $n = de$, $\gcd(d, e) = 1$ and $\mathrm{ord}_e(k) = d$. Conversely, any choice of d, e and k satisfying these conditions gives a group $G(d, e, k)$ of order n. Moreover, two such groups $G(d, e, k)$ and $G(d', e', k')$ are isomorphic if and only if $d = d'$, $e = e'$, and k, k' generate the same cyclic subgroup of $U(e)$.

Proof. This follows from [MM84, Lemmas 3.5 & 3.6]. □

Remark 3.1.3. The existence of k with $\mathrm{ord}_e(k) = d$ implies that d divides $\varphi(e) = |U(e)|$. Thus there may be many factorisations $n = de$ of n for which no groups $G(d, e, k)$ occur.

Remark 3.1.4. We note in passing how Hölder's formula (3.1) follows from Lemma 3.1.2. For fixed d and e, the number of isomorphism types of group $G(d, e, k)$ is the number of (necessarily cyclic) subgroups of order d in $U(e)$. Each such group is the product of its Sylow $p-$subgroups for the primes p dividing d. For each such p, the $p-$rank of $U(e)$ is $v(p, e)$, so $U(p)$ contains $(p^{v(p,e)} - 1)/(p - 1)$ subgroups of order p. Taking the product over p gives the number of subgroups of order d. Summing over d yields the formula (3.1) for the number of isomorphism types of groups of order n.

Proposition 3.1.5. Let $G = G(d, e, k)$ be a group of squarefree order n as in Lemma 3.1.2. Let $z = \gcd(e, k-1)$ and $g = e/z$, so that we have factorisations $e = gz$ and $n = de = dgz$. Then the centre $Z(G)$ of G is the cyclic group $\langle \sigma^g \rangle$ of order z, and the commutator subgroup G' of G is the the cyclic group $\langle \sigma^z \rangle$ of order g.

Proof. For $\gamma = \sigma^a \tau^b \in G$, we have $\sigma^{-1}\gamma\sigma = \sigma^{a-1+k^b}\tau^b$. Since $\mathrm{ord}_e(k) = d$, it follows that γ commutes with σ if and only if $d \mid b$. But then $\gamma = \sigma^a$ and $\tau\gamma\tau^{-1} = \tau\sigma^a\tau^{-1} = \sigma^{ak}$. Thus $\tau\gamma\tau^{-1} = \gamma$ precisely when $e \mid a(k-1)$, that is, when $g \mid a$. Hence $Z(G) = \langle \sigma^g \rangle$.

Turning to G', we have $\tau\sigma\tau^{-1}\sigma^{-1} = \sigma^{k-1}$. Thus G' contains the normal subgroup $\langle \sigma^{k-1} \rangle = \langle \sigma^z \rangle$ of G. Equality holds since $G/\langle \sigma^{k-1} \rangle$ is abelian. □

We next find the number of isomorphism classes of groups G corresponding to the factorisation $n = dgz$.

Proposition 3.1.6. Let $n = dgz$ be squarefree. Then the number of isomorphism types of groups G of order n with $|Z(G)| = z$ and $|G'| = g$ is

$$\varphi(d)^{-1} \sum_{f \mid g} \mu\left(\frac{g}{f}\right) \prod_{p \mid d} (p^{v(p,f)} - 1). \tag{3.2}$$

Proof. We keep d and $e = n/d$ fixed. For each factor g of e let $m(g)$ be the number of isomorphism types of groups $G = G(d, e, k)$ (with k varying) for which $|G'| = g$. We need to show that $m(g)$ is given by the formula (3.2).

Let $m^*(g)$ be the number of groups $G(d, e, k)$ for which $|G'|$ divides g. Then

$$m^*(g) = \sum_{f \mid g} m(f),$$

and so, by Möbius inversion,

$$m(g) = \sum_{f \mid g} m^*(f) \mu\left(\frac{g}{f}\right). \tag{3.3}$$

The distinct isomorphism types of groups G correspond to distinct subgroups D of order d in $U(e) \cong \prod_{q|e} U(q)$, where the product is over primes q dividing e. Let $f \mid e$. Then $|G'|$ divides f precisely when e/f divides $|Z(G)|$, which occurs when D has trivial projection in the factor $U(q)$ for each prime q dividing e/f. Hence $m^*(f)$ is the number of subgroups of order d in $U(f)$, and, arguing as in Remark 3.1.4, this is $\prod_{p|d}(p^{v(p,f)} - 1)/(p-1)$. Substituting into (3.3) and noting that $\prod_{p|d}(p-1) = \varphi(d)$, we obtain the expression (3.2) for $m(g)$. □

3.2 Automorphisms and the Holomorph

For this section and the next, we fix a group $G = G(d, e, k)$ of squarefree order n. We keep the preceding notation, so $g = |G'|$, $z = |Z(G)|$, and $n = de = dgz$. Our goal is to find the number of cyclic subgroups of $\mathrm{Hol}(G)$ which are regular on G. By Lemma 1.1.1, this will enable us to find the number of Hopf−Galois structures of type G on a cyclic extension of degree n. In this section, we will describe $\mathrm{Aut}(G)$ and $\mathrm{Hol}(G)$.

In this section, we consistently use the notation q for prime factors of e as either $q \mid g$ or $q \mid z$ and the notation p for prime factors of d.

We begin by recording a formula which allows us to perform calculations in G itself. For integers h and $j \geq 0$, we define

$$S(h, j) = \sum_{i=0}^{j-1} h^i. \tag{3.4}$$

In particular, $S(h, 0) = 0$. A simple induction shows that, for any $a \in \mathbb{Z}$,

$$(\sigma^a \tau)^j = \sigma^{aS(k,j)} \tau^j. \tag{3.5}$$

The next result describes the automorphisms of G.

Lemma 3.2.1. We have $|\mathrm{Aut}(G)| = g\varphi(e)$ and

$$\mathrm{Aut}(G) \cong C_g \rtimes U(e),$$

where $a \in U(e)$ acts on C_g by $x \mapsto x^a$. (Note that in general this action is not faithful.)

Explicitly, $\mathrm{Aut}(G)$ is generated by the automorphism θ and automorphisms ϕ_s for each $s \in U(e)$, where

$$\theta(\sigma) = \sigma, \qquad \theta(\tau) = \sigma^z\tau, \tag{3.6}$$

and

$$\phi_s(\sigma) = \sigma^s, \qquad \phi_s(\tau) = \tau. \tag{3.7}$$

These automorphisms satisfy the relations

$$\theta^g = \mathrm{id}_G, \qquad \phi_s\phi_t = \phi_{st}, \qquad \phi_s\theta\phi_s^{-1} = \theta^s. \tag{3.8}$$

Proof. We first verify the existence of the automorphisms θ and ϕ_s. Since $(\sigma^z\tau)\sigma(\sigma^z\tau)^{-1} = \sigma^k$, (3.6) will determine an automorphism θ provided that $\sigma^z\tau$ has order d. By (3.5), this will hold if $e \mid zS(k,d)$, that is, if $g \mid S(k,d)$. But for each prime $q \mid g$, we have $k^d \equiv 1 \not\equiv k \pmod{q}$, so that

$$S(k,d) = \frac{k^d - 1}{k - 1} \equiv 0 \pmod{q}.$$

Thus $g \mid S(k,d)$, as required. This shows the existence of the automorphism θ. For $s \in U(e)$, the element σ^s has order e and $\tau\sigma^s\tau^{-1} = (\sigma^s)^k$. It follows that there is an automorphism ϕ_s as given in (3.7).

It is clear that θ has order g. The remaining relations in (3.8) are easily verified by checking them on the generators σ, τ of G.

We have now shown that θ and the ϕ_s generate a subgroup of $\mathrm{Aut}(G)$ isomorphic to $C_g \rtimes U(e)$. This subgroup has order $g\varphi(e)$. It remains to show that there are no further automorphisms.

Let $\psi \in \mathrm{Aut}(G)$. As $\langle\sigma\rangle$ is a characteristic subgroup of G, being the unique subgroup of order e, we have $\psi(\sigma) = \sigma^s$ for some $s \in U(e)$. Let $\psi(\tau) = \sigma^a\tau^b$ with $0 \le b < d$. Since ψ must satisfy $\psi(\tau)\psi(\sigma)\psi(\tau)^{-1} = \psi(\sigma)^k$, we have $\sigma^{sk^b} = \sigma^{sk}$ and hence $b = 1$. Thus, by (3.5) again,

$$\psi(\tau)^d = \sigma^{aS(k,d)},$$

so that $aS(k,d) \equiv 0 \pmod{e}$. In particular, for each prime q dividing z, we have $q \mid aS(k,d)$. But $S(k,d) \equiv d \not\equiv 0 \pmod{q}$ since $k \equiv 1 \pmod{q}$. Thus $q \mid a$. It follows that $a = zc$ for some $c \in \mathbb{Z}$, so $\psi = \theta^c\phi_s$. □

We now consider the holomorph $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$ of G. We write an element of this group as $[\alpha, \psi]$, where $\alpha \in G$ and $\psi \in \mathrm{Aut}(G)$. The multiplication in $\mathrm{Hol}(G)$ is given by

$$[\alpha, \psi][\alpha', \psi'] = [\alpha\psi(\alpha'), \psi\psi']. \tag{3.9}$$

(The subgroup G in $\mathrm{Hol}(G)$ is therefore identified with the left translations in $\mathrm{Perm}(G)$.) In view of Lemma 3.2.1, an arbitrary $x \in \mathrm{Hol}(G)$ can be written $x = [\sigma^a\tau^b, \theta^c\phi_s]$, where $a \in \mathbb{Z}_e$, $s \in U(e)$, $b \in \mathbb{Z}_d$ and $c \in \mathbb{Z}_g$. In Lemma 3.2.2 below, we will give a formula for powers of x in the special case $b = 1$. We will then show in Proposition 3.2.3 why this case is all we need. We first introduce some further notation.

Define

$$T(k,s,j) = \sum_{h=0}^{j-1} S(s,h)k^{h-1} \text{ for } j \ge 1, \qquad T(k,s,0) = 0, \tag{3.10}$$

where $S(s,h)$ is given by (3.4). Note that we then have $T(k,s,1) = 0$ and

$$T(k,s,j+1) = T(k,s,j) + k^{j-1}S(s,j) \text{ for } j \ge 0.$$

Lemma 3.2.2. Let $x = [\sigma^a\tau, \theta^c\phi_s]$. Then, for $j \geq 0$, we have

$$x^j = [\sigma^{A(j)}\tau^j, \theta^{cS(s,j)}\phi_{s^j}] \tag{3.11}$$

where

$$A(j) = aS(sk, j) + czkT(k, s, j). \tag{3.12}$$

Proof. We argue by induction on j. When $j = 0$, we have $S(s, 0) = T(k, s, 0) = 0$ and $A(0) = 0$, so (3.11) holds in this case. Assuming (3.11) for j, we have from (3.9) that

$$\begin{aligned} x^{j+1} &= [\sigma^{A(j)}\tau^j, \theta^{cS(s,j)}\phi_{s^j}][\sigma^a\tau, \theta^c\phi_s] \\ &= [\sigma^{A(j)}\tau^j(\theta^{cS(s,j)}\phi_{s^j}(\sigma^a\tau)), \theta^{cS(s,j)}\phi_{s^j}\theta^c\phi_s]. \end{aligned}$$

Thus, using (3.8), the second component of x^{j+1} is

$$\theta^{cS(s,j)}\phi_{s^j}\theta^c\phi_s = \theta^{cS(s,j)}\theta^{cs^j}\phi_{s^j}\phi_s = \theta^{cS(s,j+1)}\phi_{s^{j+1}},$$

as required for (3.11). As for the first component of x^{j+1}, since

$$\theta^{cS(s,j)}\phi_{s^j}(\sigma^a\tau) = \sigma^{as^j}\sigma^{czS(s,j)}\tau,$$

we have

$$\begin{aligned} \sigma^{A(j)}\tau^j(\theta^{cS(s,j)}\phi_{s^j}(\sigma^a\tau)) &= \sigma^{A(j)}\tau^j\sigma^{as^j}\sigma^{czS(s,j)}\tau \\ &= \sigma^{A(j)}\sigma^{as^jk^j}\sigma^{czS(s,j)k^j}\tau^{j+1}. \end{aligned}$$

We write this as $\sigma^{A'}\tau^{j+1}$, and calculate

$$\begin{aligned} A' &= A(j) + as^j k^j + czS(s,j)k^j \\ &= a(S(sk,j) + (sk)^j) + czk[T(k,s,j) + k^{j-1}S(s,j)] \\ &= aS(sk,j+1) + czkT(k,s,j+1) \\ &= A(j+1). \end{aligned}$$

Thus (3.11) holds with j replaced by $j+1$. This completes the induction. □

Proposition 3.2.3. Let C be a cyclic subgroup of $\mathrm{Hol}(G)$ which is regular on G. Then C is generated by some element

$$x = [\sigma^a\tau, \theta^c\phi_s],$$

in which τ occurs with exponent 1. In fact, C contains precisely $\varphi(e)$ generators of this type.

Proof. For any $\psi \in \mathrm{Aut}(G)$ and arbitrary $\alpha = \sigma^a\tau^b \in G$, we have $\psi(\alpha) = \sigma^{a'}\tau^b$ for some $a' \in \mathbb{Z}$. This is clear from Lemma 3.2.1 as it holds for $\psi = \phi_s$ and $\psi = \theta$. It then follows from (3.9) that the function $\mathrm{Hol}(G) \longrightarrow \langle\tau\rangle$, given by $[\sigma^a\tau^b, \psi] \mapsto \tau^b$, is a group homomorphism. (This is not automatic, since the function $\mathrm{Hol}(G) \longrightarrow G$ given by $[\sigma^a\tau^b, \psi] \mapsto \sigma^a\tau^b$, is not in general a homomorphism.) In particular, for any $x = [\sigma^a\tau^b, \theta^c\phi_s] \in \mathrm{Hol}(G)$ and any $j \geq 1$, we have $x^j = [\sigma^A\tau^{bj}, \psi]$ for some $A \in \mathbb{Z}_e$ and some $\psi \in \mathrm{Aut}(G)$, both depending on j. The permutation x^j of G takes 1_G to $\sigma^A\tau^{bj}$.

Now let C be a regular cyclic subgroup of $\mathrm{Hol}(G)$, and let $x = [\sigma^a\tau^b, \theta^c\phi_s]$ be a generator. Thus x has order n. Since C is transitive on G, the elements $\sigma^A\tau^{bj}$, as j varies, must run through all elements of G. In particular, bj must run through all residue classes modulo d. Hence $\gcd(b,d) = 1$, and there exists $f \geq 1$ with $bf \equiv 1 \pmod{d}$. Since $\gcd(d,e) = 1$, we may further assume that $\gcd(f,e) = 1$. Then $\gcd(f,n) = 1$, so

that x^f is also a generator of C, and $x^f = [\sigma^{A'}\tau^{bf}, \psi'] = [\sigma^{A'}\tau, \psi']$ for some A' and ψ'. Replacing x by x^f, we have found a generator of C with $b = 1$, as required.

Now let x be any such generator. Then x^j will be another if and only if $\gcd(j, n) = 1$ and $j \equiv 1 \pmod{d}$. The number of such generators is therefore $\varphi(n)/\varphi(d) = \varphi(e)$. $\square$

Chapter 4

Cyclic Extensions of Squarefree Degree

In this chapter, we investigate Hopf−Galois structures on a cyclic field extension L/K of an arbitrary squarefree degree n. Thus we consider cyclic extensions whose degree has a prime factorisation at the other extreme to those treated in [Koh98]. By a result of Greither and Pareigis, each such Hopf−Galois structure corresponds to a group of order n, whose isomorphism class we call the type of the Hopf−Galois structure. We show that every group of order n can occur, and we determine the number of Hopf−Galois structures of each type. We then express the total number of Hopf−Galois structures on L/K as a sum over factorisations of n into three parts. As examples, we give closed expressions for the number of Hopf−Galois structures on a cyclic extension whose degree is a product of three distinct primes (There are several cases, depending on congruence conditions between the primes.) We also consider one case where the degree is a product of four primes.

We will discuss Hopf−Galois structures on arbitrary Galois extensions of squarefree degree in Chapter 5.

4.1 Introduction and Statement of Main Results

The type of a Hopf−Galois structure on a cyclic extension of squarefree degree n could potentially be any group G of order n. There may be many of these. Indeed, Hölder

[Höl95] showed by (3.1) the number of isomorphism types of groups of squarefree order n.

It is an immediate consequence of Theorem 4.1.1 below that, for each group G of order n, the number of Hopf–Galois structures of type G on a cyclic extension of degree n cannot be zero. Thus all possible types do in fact occur. The cyclic extensions of squarefree degree therefore form a class for which both the number of distinct types of Hopf–Galois structures on a given extension, and the number of distinct prime factors of the degree of a given extension, may be arbitrarily large. To the best of our knowledge, this is the first class of extensions with these properties for which it has been possible to enumerate all Hopf–Galois structures. For comparison, we mention that, when the Galois group Γ is a nonabelian simple group, the number of prime factors of $|\Gamma|$ may be arbitrarily large, but there are only two Hopf–Galois structures, both of type Γ [Byo04a]. On the other hand, for Galois extensions of degree $p_1p_2p_3$, where p_1, p_2, p_3 are distinct odd primes satisfying certain congruence conditions, Kohl [Koh16] has determined all Hopf–Galois structures for each possible Galois group. In this case, the number of distinct types may be arbitrarily large, but the number of primes dividing the degree is of course fixed at three.

We see in Proposition 3.1.5 that each group G of squarefree order n gives rise to a factorisation $n = dgz$ of n, in which g (respectively, z) is the order of the commutator subgroup G' (respectively, the centre $Z(G)$) of G. We can now state the first of the two main results of this chapter.

Theorem 4.1.1. Let L/K be a cyclic extension of fields of squarefree degree n, and let G be any group of order n. Let $z = |Z(G)|$, $g = |G'|$ and $d = n/(gz)$. Then L/K admits precisely $2^{\omega(g)}\varphi(d)$ Hopf–Galois structures of type G, where φ is Euler's totient function and $\omega(g)$ is the number of (distinct) prime factors of g.

Our second result gives the total number of Hopf–Galois structures.

Theorem 4.1.2. The number of Hopf−Galois structures on a cyclic field extension of squarefree degree n is

$$\sum_{dgz=n} 2^{\omega(g)}\mu(z)\prod_{p|d}\left(p^{v(p,g)}-1\right), \tag{4.1}$$

where the product is over ordered triples (d,g,z) of natural numbers with $dgz=n$. Here μ is the Möbius function.

We remark that (4.1) has a similar shape to Hölder's formula (3.1), although with a sum over factorisations into three parts rather than two. In both cases, the term for each factorisation involves a product over primes p dividing d, in which the contribution corresponding to p does not depend on d and p alone. (In (3.1) it depends on e, and in (4.1) on g.)

In §4.2, we determine all regular cyclic subgroups in $\mathrm{Hol}(G)$ and complete the proof of Theorem 4.1.1. In §4.3, we sum over the different isomorphism types G to prove Theorem 4.1.2.

Until the end of §4.3, we shall systematically use the notation p for prime factors of d and q for prime factors of e. Thus the primes q are of two types: either $q \mid g$ or $q \mid z$.

4.2 Hopf−Galois structures of type G

For this section, we fix a group $G = G(d,e,k)$ of squarefree order n. Then as a first step towards determining when the element x in Proposition 3.2.3 generates a regular subgroup, we give a condition for transitivity.

Lemma 4.2.1. Let $x = [\sigma^a\tau, \theta^c\phi_s] \in \mathrm{Hol}(G)$. Then the subgroup $\langle x\rangle$ of $\mathrm{Hol}(G)$ acts transitively on G if and only if $\langle x^d\rangle$ acts transitively on $\langle\sigma\rangle$.

Proof. Let $\langle x\rangle$ be transitive on G. Then, for each $i \in \mathbb{Z}$, there is some j such $x^j \cdot 1_G = \sigma^i$. Then $d \mid j$ by (3.11). Thus $\langle x^d\rangle$ acts transitively on $\langle\sigma\rangle$. Conversely, suppose that $\langle x^d\rangle$

acts transitively on $\langle\sigma\rangle$. Let $\sigma^i\tau^j \in G$. By Lemma 3.2.2, we have $x^{-j} \cdot \sigma^i\tau^j \in \langle\sigma\rangle$. As $\langle x^d\rangle$ is transitive on $\langle\sigma\rangle$, there is some $h \in \mathbb{Z}$ with $x^{dh-j} \cdot \sigma^i\tau^j = 1_G$. Thus the arbitrary element $\sigma^i\tau^j$ lies in the same orbit under $\langle x\rangle$ as 1_G, so that $\langle x\rangle$ is transitive on G. □

In order to study the orbits of $\langle x^d\rangle$ on $\langle\sigma\rangle$, we examine the congruence properties of the sums $S(k,j)$ and $T(k,s,j)$ defined in (3.4) and (3.10) when j is a multiple of d.

Proposition 4.2.2. Let q be a prime dividing e. In the following, all congruences are modulo q. We will omit the modulus for brevity. Abusing notation, we will write $\frac{u}{v}$ in such a congruence to denote uv^* where $vv^* \equiv 1$. (This notation will only be used when $v \not\equiv 0$.)

(i) For any s, $i \in \mathbb{Z}$ with $i \geq 0$, we have

$$S(s, di) \equiv \begin{cases} di & \text{if } s \equiv 1; \\ \\ \dfrac{s^{di}-1}{s-1} & \text{otherwise.} \end{cases} \tag{4.2}$$

(ii) Recall that $k^d \equiv 1$. If also $k \not\equiv 1$ then, for any s, $i \in \mathbb{Z}$ with $i \geq 0$, we have

$$T(k, s, di) \equiv \begin{cases} \dfrac{di}{k(k-1)} & \text{if } s \equiv 1; \\ \\ \dfrac{di}{k(s-1)} & \text{if } sk \equiv 1; \\ \\ \dfrac{(s^{di}-1)}{k(s-1)(sk-1)} & \text{otherwise.} \end{cases} \tag{4.3}$$

Proof. (i) This is immediate.

(ii) The case $i = 0$ is clear, so assume $i \geq 1$. First let $s \equiv 1$. Then $S(s, j) \equiv j$, so

$$\begin{aligned}
(k-1)T(k,s,di) &= \sum_{j=0}^{di-1}(k-1)jk^{j-1} \\
&= \sum_{j=0}^{di-1} jk^j - \sum_{j=1}^{di-1} jk^{j-1} \\
&= \sum_{j=0}^{di-1} jk^j - \sum_{j=0}^{di-2}(j+1)k^j \\
&= \sum_{j=0}^{di-1} jk^j - \sum_{j=0}^{di-1}(j+1)k^j + dik^{di-1} \\
&= -\sum_{j=0}^{di-1} k^j + dik^{di-1}.
\end{aligned}$$

As $k^d \equiv 1 \not\equiv k$, we then have

$$(k-1)T(k,s,di) \equiv dik^{di-1},$$

giving the result for $s \equiv 1$.

If $s \not\equiv 1$ then

$$\begin{aligned}
T(k,s,di) &\equiv \sum_{j=0}^{di-1}\left(\frac{s^j-1}{s-1}\right)k^{j-1} \\
&\equiv \frac{1}{k(s-1)}\left[\sum_{j=0}^{di-1}(sk)^j - \sum_{j=0}^{di-1}k^j\right].
\end{aligned}$$

The second sum vanishes mod q. The first is congruent to di if $sk \equiv 1$, giving the result

in this case. Finally if $sk \not\equiv 1 \not\equiv s$ then

$$\begin{aligned} T(k,s,di) &\equiv \frac{1}{k(s-1)} \sum_{j=0}^{di-1} (sk)^j \\ &\equiv \frac{1}{k(s-1)(sk-1)} \left((sk)^{di} - 1 \right) \\ &\equiv \frac{1}{k(s-1)(sk-1)} \left(s^{di} - 1 \right). \end{aligned}$$

□

Lemma 4.2.3. Let $x = [\sigma^a \tau, \theta^c \phi_s] \in \mathrm{Hol}(G)$, so $a \in \mathbb{Z}_e$, $c \in \mathbb{Z}_g$, $s \in U(e)$. Then x generates a regular cyclic subgroup of $\mathrm{Hol}(G)$ if and only if the triple (s,a,c) satisfies the following conditions:

(i) for each prime $q \mid z$, we have $s \equiv 1 \pmod{q}$ and $q \nmid a$;

(ii) for each prime $q \mid g$, either

$$s \equiv 1 \pmod{q} \text{ and } c \not\equiv 0 \pmod{q}, \text{ or}$$

$$s \equiv k^{-1} \pmod{q} \text{ and } (s-1)a + cz \not\equiv 0 \pmod{q}.$$

Proof. Suppose that $\langle x \rangle$ is regular, and hence transitive, on G. By Lemma 4.2.1, $\langle x^d \rangle$ is transitive on $\langle \sigma \rangle$. It follows using Lemma 3.2.2 that the expression

$$A(di) = aS(sk, di) + czkT(k,s,di)$$

represents all residue classes mod e as i varies. In particular, $A(di)$ represents every residue class mod q for each prime factor q of e. We investigate this condition for each q in turn. Again, we omit the modulus in congruences modulo q.

First, let $q \mid z$, so $k \equiv 1$. If $s \not\equiv 1$, then $sk \not\equiv 1$, so by Proposition 4.2.2(i) we

have

$$A(di) \equiv \frac{a(s^{di}-1)}{s-1},$$

which cannot represent all residue classes mod q since there is no i such that $s^{di} \equiv 0$. On the other hand, if $s \equiv 1$ then

$$A(di) \equiv adi. \tag{4.4}$$

Since $q \nmid d$, this represents all residue classes mod q precisely when $q \nmid a$. Thus (i) holds.

Now let $q \mid g$, so $k \not\equiv 1$ but $k^d \equiv 1$. If $s \not\equiv 1$ and $s \not\equiv k^{-1}$, then, using both parts of Proposition 4.2.2, we have

$$\begin{aligned} A(di) &\equiv \left(\frac{(sk)^{di}-1}{sk-1}\right) a + czk \left(\frac{s^{di}-1}{k(s-1)(sk-1)}\right) \\ &= \frac{(s^{di}-1)}{(s-1)(sk-1)} \left((s-1)a + cz\right). \end{aligned}$$

Again, this cannot represent all residue classes mod q since $s^{di} \not\equiv 0$.

It remains to consider the two special cases $s \equiv 1 \not\equiv k$ and $s \equiv k^{-1} \not\equiv 1$.

If $s \equiv 1 \not\equiv k$ then, as $(sk)^d \equiv k^d \equiv 1$, we have

$$A(di) \equiv czk \left(\frac{di}{k(k-1)}\right) = \frac{czdi}{k-1}. \tag{4.5}$$

As $q \nmid zd$, this represents all residue classes mod q precisely when $q \nmid c$, giving the first case in (ii).

If $s \equiv k^{-1} \not\equiv 1$ then

$$\begin{aligned} A(di) &\equiv adi + czk\left(\frac{di}{k(s-1)}\right) \\ &\equiv \frac{di}{s-1}\left((s-1)a + cz\right). \end{aligned} \tag{4.6}$$

This represents all residue classes mod q precisely when $(s-1)a + cz \not\equiv 0$, giving the second case in (ii).

We have now shown that if x generates a regular cyclic subgroup, then (i) and (ii) hold.

Conversely, suppose that (i) and (ii) hold. Then, by Proposition 4.2.2, the congruences (4.4), (4.5) and (4.6) hold modulo all relevant q. For each prime $q \mid e$, we then have that $A(di)$ represents all residue classes mod q as i runs through any complete set of residues mod q. By the Chinese Remainder Theorem, $A(di)$ then ranges through all residue classes mod e as i does. By Lemma 3.2.2, $\langle x^d \rangle$ is then transitive on $\langle \sigma \rangle$, so $\langle x \rangle$ is transitive on G by Lemma 4.2.1. Finally, (4.4), (4.5) and (4.6) show that $A(de) \equiv 0 \pmod{e}$, so that $x^n = 1_G$. Hence $\langle x \rangle$ is regular on G. □

Proof of Theorem 4.1.1. By Proposition 3.2.3, any regular cyclic subgroup of $\mathrm{Hol}(G)$ is generated by an element x as in Lemma 4.2.3. We count the number of triples (s, a, c) satisfying the conditions there. As there is only one possibility for $s \bmod q$ when $q \mid z$ but two when $q \mid g$, there are $2^{\omega(g)}$ possibilities for $s \pmod{e}$. Let us fix s and consider the possibilities for a and c. For each prime $q \mid z$, condition (i) in Lemma 4.2.3 excludes one possibility for $a \bmod q$. For each $q \mid g$, we may choose $a \bmod q$ arbitrarily, and then, in either case of condition (ii), one possibility for $c \bmod q$ is excluded. Thus we have $\varphi(z)g$ choices for $a \bmod e$, and then $\varphi(g)$ choices for $c \bmod g$. The number of elements $x = [\sigma^a\tau, \theta^c\phi_s]$ which generate a regular subgroup is therefore $2^{\omega(g)}\varphi(z)g\varphi(g)$. By Proposition 3.2.3, each regular cyclic subgroup contains $\varphi(e) = \varphi(z)\varphi(g)$ such

generators, so there are $2^{\omega(g)}g$ of these subgroups. Thus, using Lemma 1.1.1 and Lemma 3.2.1 (and writing C_n for the cyclic group of order n), we find that the number of Hopf−Galois structures of type G is

$$\frac{|\mathrm{Aut}(C_n)|}{|\mathrm{Aut}(G)|}\,2^{\omega(g)}g = \frac{\varphi(n)}{g\varphi(e)}2^{\omega(g)}g = 2^{\omega(g)}\varphi(d).$$

□

4.3 Proof of Theorem 4.1.2

In this section, we obtain the total number of Hopf−Galois structures on a cyclic field extension of squarefree degree n, thereby completing the proof of Theorem 4.1.2.

For each factorisation $n = dgz$, we have seen in Proposition 3.1.6 that the number of corresponding isomorphism types of group G is

$$\varphi(d)^{-1}\sum_{f|g}\mu\left(\frac{g}{f}\right)\prod_{p|d}(p^{v(p,f)}-1).$$

We have also seen in Theorem 4.1.1 that there $2^{\omega(g)}\varphi(d)$ Hopf−Galois structures of each of these types. To obtain the total number of Hopf− Galois structures, we simply multiply these two quantities and sum over factorisations of n. This yields

$$\sum_{dgz=n}2^{\omega(g)}\varphi(d)\left(\varphi(d)^{-1}\sum_{f|g}\mu\left(\frac{g}{f}\right)\prod_{p|d}(p^{v(p,f)}-1)\right).$$

Setting $t = g/f$ and noting that $\omega(g) = \omega(t) + \omega(f)$, we can rewrite the previous sum as

$$\sum_{dftz=n}\mu(t)2^{\omega(t)}2^{\omega(f)}\prod_{p|d}(p^{v(p,f)}-1).$$

Let $m = tz$, and observe that $\mu(t) = (-1)^{\omega(t)}$. The sum then becomes

$$\sum_{df\, m=n} \left(\sum_{t|m} (-2)^{\omega(t)} \right) 2^{\omega(f)} \prod_{p|d} (p^{v(p,f)} - 1).$$

Recall that a function F on the natural numbers is said to be multiplicative if $F(rs) = F(r)F(s)$ whenever $\gcd(r, s) = 1$. The function $t \mapsto (-2)^{\omega(t)}$ is clearly multiplicative, and hence so is the function $m \mapsto \sum_{t|m}(-2)^{\omega(t)}$. However, evaluating this last function at a prime q gives $(-2)^{\omega(1)} + (-2)^{\omega(q)} = 1 + (-2) = -1 = \mu(q)$. As μ is also multiplicative, it follows that $\sum_{t|m}(-2)^{\omega(t)} = \mu(m)$ for squarefree m. (This is not true for arbitrary natural numbers m.) Hence the total number of Hopf−Galois structures on a cyclic extension of squarefree degree n is

$$\sum_{df\, m=n} \mu(m) 2^{\omega(f)} \prod_{p|d} (p^{v(p,f)} - 1).$$

After a change of notation, this gives the formula (4.1), completing the proof of Theorem 4.1.2.

4.4 Examples

In this section, we give some examples and show how several results in the literature can be obtained as special cases of our results. Throughout, n is a squarefree integer and L/K is a cyclic Galois extension of degree n.

4.4.1 Cyclic Hopf-Galois Structures

The group $G(d, e, k)$ in Lemma 3.1.2 is cyclic only when $d = 1$, $e = n$. Indeed, this is the only case where $G(d, e, k)$ is abelian, or even nilpotent. In this case $z = n$, $g = 1$, and Theorem 4.1.1 shows that there is only one Hopf−Galois structure of cyclic (or abelian, or nilpotent) type on L/K. This can also be seen from [Byo13, Theorem 2]. The unique cyclic Hopf−Galois structure is of course the classical one.

When $\gcd(n, \varphi(n)) = 1$, there are no other groups $G(d, e, k)$, and hence there are no Hopf−Galois structures on L/K beyond the classical one. This was shown, together with its converse, in [Byo96]. The case that n is prime occurs in [Chi89].

4.4.2 Dihedral Hopf-Galois Structures

Let $n = 2m$ where m is an odd squarefree number. The group $G(d, e, k)$ in Lemma 3.1.2 is dihedral when $d = 2$ and $k = -1 \in U(e)$. Then $e = g = m$. It follows from Theorem 4.1.1 that a cyclic extension of degree n admits $2^{\omega(m)}$ Hopf−Galois structures of dihedral type.

4.4.3 Two Primes

Let $n = pq$ for primes $p > q$. We assume that $q \mid (p-1)$ (since otherwise the only group of order n is the cyclic group C_n). Up to isomorphism, there are two groups of order n, the cyclic group C_n (with $d = 1$, $g = 1$, $e = z = pq$) and the metabelian group $M = C_p \rtimes C_q$ where C_q acts nontrivially on C_p (so $d = q$, $e = g = p$, $z = 1$). As we have seen in §4.4.1, a cyclic extension of degree n admits just one Hopf−Galois structure of cyclic type (namely the classical one). By Theorem 4.1.1, it also admits $2^{\omega(p)}\varphi(q) = 2(q-1)$ Hopf−Galois structures of type M. This result was obtained in [Byo04b], where Hopf−Galois structures on a Galois extension with Galois group M were also considered. When $q = 2$, the result follows from §4.4.2.

Table 4.1: Nonzero terms in (4.1) for $n = pq$.

d	g	z	Term in (4.1)
1	pq	1	4
1	p	q	-2
1	q	p	-2
1	1	pq	1
q	p	1	$2(q-1)$

Let us also verify that Proposition 3.1.6 correctly counts the isomorphism types corresponding to each factorisation $n = dgz$, and that Theorem 4.1.2 correctly counts the total number of Hopf−Galois structures, in this case.

In the sum (3.2) of Proposition 3.1.6, $\prod_{p|d}(p^{v(p,f)} - 1)$ vanishes unless $d = 1$ or $d = q$, $f = p$ (so that also $g = p$). When $d = 1$, (3.2) reduces to

$$\sum_{f|g} \mu\left(\frac{g}{f}\right) = \begin{cases} 1 & \text{if } g = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Thus when $d = 1$, to get a group $G(d, e, k)$ we must take $g = 1$ and $z = pq$. We then have $G(d, e, k) = C_n$. When $d \neq 1$, all terms in (3.2) vanish unless $d = q$, $g = p$, when the term for $f = p$ gives $\varphi(q)^{-1}(q^1 - 1) = 1$. Thus (3.2) tells us that there is just one isomorphism type of nonabelian group of order n. Hence Proposition 3.1.6 does indeed give the correct number of isomorphism types for each factorisation. By similar reasoning (which we leave to the reader), Hölder's formula (3.1) correctly predicts two isomorphism classes of groups of order n.

We now turn to Theorem 4.1.2. The product over $p \mid d$ vanishes unless $d = 1$ or $d = q$, $g = p$. The nonzero contributions to (4.1) for the various factorisations $n = gzd$ are shown in Table 4.1. Summing the final column of Table 4.1 gives the correct count of $2(q - 1) + 1$ Hopf−Galois structures on a cyclic extension of degree $n = pq$. Table 4.1 also illustrates an important feature of the formula (4.1): factorisations $n = dgz$ for which there are no corresponding groups G can nevertheless contribute nonzero terms to (4.1).

4.4.4 Three Primes

Let $n = p_1p_2p_3$ where $p_1 < p_2 < p_3$ are primes. Both the number of isomorphism classes of groups of order n, and the number of Hopf−Galois structures on a cyclic extension

of degree n, depend on congruence conditions relating the three primes. There are two combinations of these conditions for which the Hopf–Galois structures on all Galois extensions of degree $p_1p_2p_3$ (not just cyclic extensions) have been enumerated.

The first of these is when $p_1 = 2$ and $p_3 = 2p_2 + 1$ (so p_2 is a Sophie Germain prime and p_3 is a safeprime). Kohl [Koh13, Theorem 5.1] treated this case as an application of his method for studying Hopf–Galois structures on Galois extensions of degree mp (with p prime and $m < p$). Those extensions with Galois group $\mathrm{Hol}(C_{p_3}) = C_{p_3} \rtimes C_{p_3-1}$ had previously been considered in [Chi03].

The second situation where all Hopf–Galois structures have been determined is when $p_1 > 2$ and $p_2 \equiv p_3 \equiv 1 \pmod{p_1}$ but $p_3 \not\equiv 1 \pmod{p_2}$. This case is treated in [Koh16, Theorem 2.4]. The same techniques could be applied to other combinations of congruence conditions, but separate calculations would be required for each case.

In the following, we will apply Theorem 4.1.1 to count the Hopf–Galois structures only on a *cyclic* extension of degree $n = p_1p_2p_3$, but under all possible combinations of congruence conditions. In particular, this will recover those parts of Kohl's results in [Koh13, Koh16] which relate to cyclic extensions.

In Table 4.2 we show the factorisations $n = dgz$ for which groups exist, the number of isomorphism types of these groups, and the number of Hopf–Galois structures of each isomorphism type.

The first column of Table 4.2 numbers the factorisations for ease of reference, and the factorisation is shown in the next 3 columns. The 5th column shows the congruence conditions which must be satisfied for groups to exist. The 6th column shows the number of isomorphism types of group corresponding to the given factorisation, as

Table 4.2: Numbers of isomorphism types and Hopf−Galois structures for $n = p_1p_2p_3$.

Case	d	g	z	Condition	# groups	# HGS per group
1	1	1	$p_1p_2p_3$		1	1
2	p_1	p_2	p_3	$p_2 \equiv 1 \pmod{p_1}$	1	$2(p_1-1)$
3	p_1	p_3	p_2	$p_3 \equiv 1 \pmod{p_1}$	1	$2(p_1-1)$
4	p_1	p_2p_3	1	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	p_1-1	$4(p_1-1)$
5	p_2	p_3	p_1	$p_3 \equiv 1 \pmod{p_2}$	1	$2(p_2-1)$
6	p_1p_2	p_3	1	$p_3 \equiv 1 \pmod{p_1p_2}$	1	$2(p_1-1)(p_2-1)$

given by Proposition 3.1.6. These can also be found directly, as explained below. The final column shows the number of Hopf−Galois structures for each isomorphism type. This is given by the formula $2^{\omega(g)}\varphi(d)$ of Theorem 4.1.1.

We now explain how to find the values in the 6th column of Table 4.2 directly. (This illustrates in simple cases the proof of Proposition 3.1.6.) Consider for example case 2, where $d = p_1$, $g = p_2$, $z = p_3$, so $e = p_2p_3$. The distinct isomorphism types of groups $G(d, e, k)$ with these parameters correspond to subgroups $\langle k \rangle \subseteq U(p_2p_3)$ of order p_1 for which $z = \gcd(k-1, p_2p_3) = p_3$. Since $k \equiv 1 \pmod{p_3}$, we can identify $\langle k \rangle$ with a subgroup of order p_1 in $U(p_2)$. Such a subgroup exists since $p_2 \equiv 1 \pmod{p_1}$, and it is unique since $U(p_2)$ is cyclic. Thus there is just one group $G(d, e, k)$ in case 2. In case 4, however, where $d = p_1$, $g = p_2p_3$ and $z = 1$, the isomorphism types of groups $G(d, e, k)$ correspond to subgroups $\langle k \rangle \subseteq U(p_2p_3)$ of order p_1 with $\gcd(k-1, p_2p_3) = 1$. Now $U(p_2p_3) \cong U(p_2) \times U(p_3)$ contains $p_1 + 1$ subgroups of order p_1. For one of these, $\gcd(k-1, p_2p_3) = p_3$. This gives the group G just found in case 2. Another of the subgroups has $\gcd(k-1, p_2p_3) = p_2$, and this is counted in case 3. The remaining $p_1 - 1$ subgroups of $U(p_2p_3)$ give groups G with $g = p_2p_3$ and $z = 1$. Thus the number of groups recorded in case 4 is $p_1 - 1$.

We now find the total number of Hopf−Galois structures on a cyclic extension of degree n, treating each combination of relevant congruence conditions on p_1, p_2, p_3 separately. The results are shown in Table 4.3. For each combination of congruence conditions, we

Table 4.3: Total numbers of Hopf–Galois structures for $n = p_1p_2p_3$.

$p_2 \mid (p_3 - 1)$	$p_1 \mid (p_3 - 1)$	$p_1 \mid (p_2 - 1)$	Cases	# groups	Total # HGS
no	no	no	1	1	1
no	no	yes	1, 2	2	$2p_1 - 1$
no	yes	no	1, 3	2	$2p_1 - 1$
no	yes	yes	1, 2, 3, 4	$p_1 + 2$	$(2p_1 - 1)^2$
yes	no	no	1, 5	2	$2p_2 - 1$
yes	no	yes	1, 2, 5	3	$2p_1 + 2p_2 - 3$
yes	yes	no	1, 3, 5, 6	4	$2p_1p_2 - 1$
yes	yes	yes	1, 2, 3, 4, 5, 6	$p_1 + 4$	$4p_1^2 + 2p_1p_2 - 6p_1 + 1$

pick out the cases from Table 4.2 where any groups $G(d, e, k)$ exist. To obtain the total number of isomorphism types of groups of order n, we add the numbers of groups from the corresponding rows in Table 4.2, giving the entries in the 5th column of Table 4.3. These agree with the values given by Kohl [Koh16, p. 46]. To obtain the total number of Hopf–Galois structures, we multiply the entries in the final two columns of Table 4.2 and add these values for the appropriate rows. After simplification, this gives the entries in the final column of Table 4.3.

We now specialise to the two situations considered in [Koh13, Theorem 5.1] and [Koh16, Theorem 2.4] in order to confirm that we recover those parts of Kohl's results pertaining to cyclic extensions.

First let $p_1 = 2$ and let $p_3 = 2p_2 + 1$ be a safeprime. Thus we have $p_j \equiv 1 \pmod{p_i}$ whenever $1 \leq i \leq j \leq 3$, corresponding to the final row ("yes–yes–yes") in our Table 4.3. The first row of the table in [Koh13, Theorem 5.1] shows that there are 6 isomorphism types of groups of order $n = p_1p_2p_3$, which Kohl denotes by C_{mp}, $C_p \times D_q$, $F \times C_2$, $C_q \times D_p$, D_{pq}, $\mathrm{Hol}(C_p)$, where $q = p_2$ and $p = p_3$. These contribute 1, 2, $2(p_2 - 1)$, 2, 4, $2(p_2 - 1)$ Hopf–Galois structures respectively. The total number of Hopf–Galois structures is therefore $4p_2 + 5$. These groups are respectively those of cases 1, 2, 5, 3, 4, 6 in our Table 4.2. Putting $p_1 = 2$ in Table 4.2, we again get $4p_2 + 5$ for the total number of Hopf–Galois structures, and the number of Hopf–Galois structures

of each type shown in Table 4.2 agrees with Kohl's values. Thus our results recover the part of Kohl's result [Koh13, Theorem 5.1] relating to cyclic extensions of degree $2pq = 2p_2(2p_2 + 1)$.

Now let $p_1 > 2$ and $p_2 \equiv p_3 \equiv 1 \pmod{p_1}$ but $p_3 \not\equiv 1 \pmod{p_2}$, corresponding to the 4th row ("no–yes–yes") of our Table 4.3. The first row of the table in [Koh16, Theorem 2.4] shows that there are $p_1 + 2$ groups G. (Note that the final column, headed $C_{p_3p_2} \rtimes_i C_{p_1}$, corresponds to $p_1 - 1$ distinct isomorphism types, given by $1 \leq i \leq p_1 - 1$.) Of these groups, one contributes one Hopf–Galois structure, two contribute $2(p_1 - 1)$, and the rest $4(p_1 - 1)$. Thus there are in total of $(2p_1 - 1)^2$ Hopf–Galois structures. This agrees with our count in Table 4.3 and the relevant cases, 1–4, in Table 4.2. (The restriction $p_1 > 2$ turns out to be irrelevant when the Galois group is cyclic.)

4.4.5 Four Primes

As a final example, we consider the case when $n = p_1p_2p_3p_4$ is the product of 4 distinct primes, under the assumption that

$$p_j \equiv 1 \pmod{p_i} \text{ whenever } i < j. \tag{4.7}$$

(Thus we have $p_1 < p_2 < p_3 < p_4$.)

We record in Table 4.4 the number of isomorphism classes of groups $G(d, e, k)$, and the number of Hopf–Galois structures of each type, corresponding to each relevant factorisation $n = dgz$.

It follows from this table that, under the assumption (4.7), there are $p_1^2 + p_1p_2 + 2p_1 + 2p_2 + 8$ isomorphism types of groups of order $n = p_1p_2p_3p_4$, and the total number of

Table 4.4: Numbers of isomorphism types and Hopf–Galois structures for $n = p_1p_2p_3p_4$.

d	g	z	# groups	# HGS per group
1	1	$p_1p_2p_3p_4$	1	1
p_1	p_2	p_3p_4	1	$2(p_1-1)$
p_1	p_3	p_2p_4	1	$2(p_1-1)$
p_1	p_4	p_2p_3	1	$2(p_1-1)$
p_1	p_2p_3	p_4	p_1-1	$4(p_1-1)$
p_1	p_2p_4	p_3	p_1-1	$4(p_1-1)$
p_1	p_3p_4	p_2	p_1-1	$4(p_1-1)$
p_1	$p_2p_3p_4$	1	$(p_1-1)^2$	$8(p_1-1)$
p_2	p_3	p_1p_4	1	$2(p_2-1)$
p_2	p_4	p_1p_3	1	$2(p_2-1)$
p_2	p_3p_4	p_1	p_2-1	$4(p_2-1)$
p_3	p_4	p_1p_2	1	$2(p_3-1)$
p_1p_2	p_3	p_4	1	$2(p_1-1)(p_2-1)$
p_1p_2	p_4	p_3	1	$2(p_1-1)(p_2-1)$
p_1p_2	p_3p_4	1	$(p_1+1)(p_2+1)-2$	$4(p_1-1)(p_2-1)$
p_1p_3	p_4	p_2	1	$2(p_1-1)(p_3-1)$
p_2p_3	p_4	p_1	1	$2(p_2-1)(p_3-1)$
$p_1p_2p_3$	p_4	1	1	$2(p_1-1)(p_2-1)(p_3-1)$

Hopf–Galois structures is

$$4p_1^2p_2^2 + 8p_1^3 + 2p_1p_2p_3 - 16p_1^2 - 6p_1p_2 + 10p_1 - 1.$$

For example, if $n = 2 \cdot 3 \cdot 7 \cdot 43 = 1806$, or more generally, if $n = 42p_4$ for any prime $p_4 \equiv 1 \pmod{42}$, then a cyclic extension of degree n admits precisely 211 Hopf–Galois structures of 28 different types. When (4.7) does not hold, we can enumerate the Hopf–Galois structures by picking out the appropriate rows in Table 4.4, just as we did in §4.4.4.

Chapter 5

Galois Extensions of Squarefree Degree

In this chapter, we extend the methods of the previous chapter to investigate Hopf−Galois structures on an arbitrary Galois field extension L/K of squarefree degree n. So we enumerate the Hopf−Galois structures of a given type. As examples, we consider the special cases where either one of G or Γ is a cyclic or dihedral group to find the number of Hopf−Galois structures in that case.

5.1 Introduction and Main Results

Let $G = G(d, e, k)$ be a group of order $n = de$ as in Lemma 3.1.2, and let $z = \gcd(e, k-1)$, $g = e/z$, as in Proposition 3.1.5.

Also let $\Gamma = G(\delta, \epsilon, \kappa)$ be another group of order n, and let $\zeta = \gcd(\epsilon, \kappa - 1)$, $\gamma = \epsilon/\zeta$.

We will determine the regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ, and hence count the Hopf−Galois structures of type G on a Galois extension with Galois group isomorphic to Γ. Such Hopf−Galois structures exist if and only if $\gamma \mid e$, and the number of them depends in a subtle way on the intersection of the structures of G and Γ.

The precise result, given in Theorem 5.4.3, requires elaborate notation to state, so we will not include a statement at this point.

To the group G we attach the data $\{r_q : q \mid e\}$ where, for each prime $q \mid e$, we define r_q to be the order of $k \mod q$. In general, the data $\{r_q\}$ are not determined by d and e, and do not determine G up to isomorphism.

In §5.5, we fix Γ, and aggregate the Hopf−Galois structures on a Galois extension with group Γ where types give rise to a given set of data $\{r_q\}$. The number of such Hopf−Galois structures is given in Theorem 5.5.1. While in principle we could further aggregate the types to obtain an expression for the total number of Hopf−Galois structures on an extension with Galois group Γ, this leads to very complicated multiple sums which do not seem to admit any simplification. Thus we shall not give an analogue of Theorem 4.1.2 for extensions with non−cyclic Galois group Γ.

To illustrate Theorem 5.4.3, we give various examples in §5.6. In particular, we consider the cases where Γ or G is cyclic or dihedral (where Γ is cyclic, we recover Theorem 4.1.1.) We also consider the cases where $|\Gamma|$ is a product of two primes, recovering the results of Byott [Byo04b], and where $|\Gamma|$ is a product of three primes, recovering and extending results of Kohl [Koh13, Koh16] and Childs [Chi03].

5.2 The groups G and Γ

Until §5.5, we fix a group

$$G = G(d, e, k) = \langle \sigma, \tau : \sigma^e = \tau^d = 1, \tau\sigma\tau^{-1} = \sigma^k \rangle.$$

This determines the numbers g and z, where $g = e/z, z = \gcd(e, k-1)$.

Since all our calculations will take place inside the single group $\mathrm{Hol}(G)$, we view k as being given with the group G. Thus we do not allow k to vary.

We will investigate regular subgroups in $\mathrm{Hol}(G)$ isomorphic to Γ, where Γ is another

group of order n. We will, as far as possible, use corresponding Greek and Roman letters for corresponding quantities for Γ and G. (For consistency with Chapter 4, we will however continue to use Greek letters to denote the generators σ, τ of G and the automorphisms θ, ϕ_s of G.) Thus we write

$$\Gamma = G(\delta, \epsilon, \kappa) = \langle S, T : S^\epsilon = T^\delta = 1, TST^{-1} = S^\kappa \rangle,$$

and set $\zeta = \gcd(\kappa - 1, \epsilon)$ and $\gamma = \epsilon/\zeta$.

It is convenient to modify the presentation of Γ. Set $X = S^\zeta$ and $Y = TS^\gamma$. As S^γ generates the centre of Γ, we have

$$\Gamma = \langle X, Y : X^\gamma = Y^{\zeta\delta} = 1, YXY^{-1} = X^\kappa \rangle. \tag{5.1}$$

Although κ is originally given as an element of $\mathbb{Z}_\epsilon^\times$, and $\kappa \equiv 1 \pmod{\zeta}$, in (5.1) we equivalently view κ as an element of $\mathbb{Z}_\gamma^\times$.
Then Γ has commutator subgroup $\Gamma' = \langle X \rangle$ of order γ.

The isomorphism class of Γ does not determine κ uniquely since we may replace κ by any other generator of the cyclic subgroup $\langle \kappa \rangle$ of $\mathbb{Z}_\gamma^\times$.

Let

$$\mathcal{K} = \{\kappa^r : r \in \mathbb{Z}_\delta^\times\}$$

be the set of such generators.
From now on, we view $\mathcal{K}$ as given (with the isomorphism class Γ) and allow κ to vary within $\mathcal{K}$.

Proposition 5.2.1. If $\mathrm{Hol}(G)$ contains any regular subgroup $\Gamma = \langle X, Y \rangle$ as in (5.1),

then $d \mid \zeta\delta$ and $\gamma \mid e$.

Moreover, the subgroup $\langle X, Y^d \rangle$ of Γ of order e acts regularly on $\langle \sigma \rangle \subseteq G$.

Proof. The projection $\mathrm{Hol}(G) \to \langle \tau \rangle$ is a group homomorphism with abelian image. This follows from (3.9) as observed in proof of Proposition 3.2.3. Thus if X and Y generate a regular subgroup Γ of $\mathrm{Hol}(G)$ then $X \in \Gamma' \subseteq \mathrm{Hol}(G)'$, so that X cannot involve τ. By regularity, some power Y^f of Y must be of the form $Y^f = [\sigma^a \tau, \psi]$ for some $\psi \in \mathrm{Aut}(G)$. Then $Y^{fj} \cdot 1_G \in \{\sigma^m : m \in \mathbb{Z}\}$ if and only if $d \mid j$. It follows that $d \mid \zeta\delta$. Since $de = n = \delta\gamma\zeta$, this is equivalent to $\gamma \mid e$. The subgroup $\langle X, Y^d \rangle$ has order e and acts without fixed points on the subset $\{\sigma^m\}$ of G, which has cardinality e. Hence this action is regular. □

Let

$$\Delta = \{r \in \mathbb{Z}_\delta^\times : r \equiv 1 \pmod{\gcd(d, \delta)}\},$$

a subgroup of $\mathbb{Z}_\delta^\times$ of order $\frac{\varphi(\delta)}{w}$, where $w = \varphi[\gcd(d, \delta)]$.

Then Δ acts on $\mathcal{K}$ without fixed points.

Let $\kappa_1, \ldots, \kappa_w$ be orbit representatives.

If $\gcd(d, \delta) = 1$ or 2 then $w = 1$.

If $\gcd(d, \delta) > 2$ then w is even and $-1 \notin \Delta$.

Thus we may assume that the orbit representatives come in mutually inverse pairs when $\gcd(d, \delta) > 2$: for each h where $1 \leq h \leq w$, $\kappa_h^{-1} \neq \kappa_h$ and κ_h^{-1} is also among the orbit representatives.

We will show that the regular subgroups in $\mathrm{Hol}(G)$ isomorphic to Γ fall into w families, and we will count the subgroups in each family.

We recall from Lemma 3.2.1 the description of the automorphisms of G.

$$\mathrm{Aut}(G) \cong C_g \rtimes \mathbb{Z}_e^\times,$$

and in particular, $|\mathrm{Aut}(G)| = g\varphi(e)$.

Explicitly, $\mathrm{Aut}(G)$ is generated by the automorphism θ and automorphisms ϕ_s for each $s \in \mathbb{Z}_e^\times$, where

$$\theta(\sigma) = \sigma, \qquad \theta(\tau) = \sigma^z \tau, \tag{5.2}$$

and

$$\phi_s(\sigma) = \sigma^s, \qquad \phi_s(\tau) = \tau. \tag{5.3}$$

These automorphisms satisfy the relations

$$\theta^g = \mathrm{id}_G, \qquad \phi_s\phi_t = \phi_{st}, \qquad \phi_s\theta\phi_s^{-1} = \theta^s. \tag{5.4}$$

Now consider a pair of elements $X, Y \in \mathrm{Hol}(G)$ of special forms with:

$$X = [\sigma^a, \theta^c], \qquad Y = [\sigma^u\tau, \theta^v\phi_t]. \tag{5.5}$$

(Thus X does not contain τ or any ϕ_s, and τ occurs with exponent 1 in Y.)

We record formulae for the powers of X and Y. Since $\theta(\sigma) = \sigma$, we have

$$X^j = [\sigma^{aj}, \theta^{cj}], \tag{5.6}$$

and from Lemma 3.2.2, we have

$$Y^j = [\sigma^{A(j)}\tau^j, \theta^{vS(t,j)}\phi_{t^j}], \tag{5.7}$$

where $A(j)$ is given by (3.12) and $S(t,j)$ is given by (3.4) as follows

$$A(j) = uS(tk, j) + zvkT(k, t, j),$$

$$S(t,j) = \sum_{i=0}^{j-1} t^i;$$

and

$$T(k,t,j) = \sum_{i=0}^{j-1} S(t,i)k^{i-1} \text{ for } j \geq 1, \qquad T(k,t,0) = 0.$$

Lemma 5.2.2. Let Γ^* be a regular subgroup of $\mathrm{Hol}(G)$ isomorphic to Γ. Then there is a unique $h \in \{1,\ldots,w\}$ such that Γ^* is generated by a pair of elements X, Y satisfying (5.5) and the relations

$$X^\gamma = Y^{\zeta\delta} = 1, \qquad YXY^{-1} = X^{\kappa_h}. \tag{5.8}$$

Indeed Γ^* contains precisely $\gamma\varphi(e)w/\varphi(\delta)$ such pairs of generators.

Proof. Since $\Gamma^* \cong \Gamma$, we can find some pair of generators X, Y satisfying the relations in (5.1). As in the proof of Proposition 5.2.1, τ can not occur in X, and there is some $f \in \mathbb{Z}$ so that τ occurs with exponent 1 in Y^f.

Then $\gcd(f,d) = 1$. Since $d \mid \zeta\delta$, we may choose f with $\gcd(f,\zeta\delta) = 1$. Thus Y^f has order $\zeta\delta$.

We replace Y by Y^f (and κ by $\kappa^f \in \mathcal{K}$). This gives a new pair of generators X, Y where Y is as in (5.5) and X has the form

$$X = [\sigma^a, \theta^c\phi_s].$$

We claim that $s = 1$, so X is also as in (5.5).

Indeed, the relations $X^\gamma = 1, YX = X^\kappa Y$ imply that $\phi_s^\gamma = 1$ and $\phi_t\phi_s = \phi_s^\kappa\phi_t$ so that $s^\gamma \equiv 1 \equiv s^{\kappa-1} \pmod{\epsilon}$.

As $\gcd(\gamma, \kappa - 1) = 1$ by the definition of γ, it follows that $s = 1$ as claimed.

Now we consider further changes to our generators X, Y which preserve the conditions (5.1) and (5.5) (except possibly for replacing κ by some other elements of $\mathcal{K}$).

So, we count the number of pairs X, Y in a given subgroup Γ^*. We may replace X by $x = X^i$ for any $i \in \mathbb{Z}_\gamma^\times$, and Y by $y = X^jY^m$ for any $j \in \mathbb{Z}_\gamma$ and $m \in \mathbb{Z}_{\zeta\delta}^\times$ with $m \equiv 1$

(mod d). (The last condition ensures that τ occurs with exponent 1 in y.) Also, we then have some other relations between x and y

$$yxy^{-1} = X^jY^mX^iY^{-m}X^{-j} = X^{i\kappa^m} = x^{\kappa^m}$$

As $\kappa \in \mathbb{Z}_\gamma^\times$ has order δ, we have

$$\{\kappa^m : m \equiv 1 \pmod{d}\} = \{\kappa^r : r \equiv 1 \pmod{\gcd(d,\delta)}\} = \{\kappa^r : r \in \Delta\}.$$

Thus we may replace X, Y by generators x, y of the form (5.5) and satisfying the relations

$$x^\gamma = y^{\zeta\delta} = 1, \qquad yx = x^{\kappa^r}y,$$

if and only if $r \in \Delta$. Hence there is a unique $h \in \{1, \dots, w\}$ so that Γ^* contains a pair of generators satisfying (5.5) and (5.8).

Finally, suppose (X, Y) is one such pair of generators. For $x = X^i, y = X^jY^m$ to be another such pair, we require

$$\kappa^m \equiv \kappa \pmod{\gamma}, \quad (X \text{ has order } \gamma),$$

so

$$m \equiv 1 \pmod{\delta}, \quad (\kappa \text{ has order } \delta).$$

We have $m \equiv 1 \pmod{d}$ and $m \equiv 1 \pmod{\delta}$ so $m \equiv 1 \pmod{\operatorname{lcm}(d,\delta)}$. But there are $\varphi(\zeta\delta)$ choices for $m \in \mathbb{Z}_{\zeta\delta}^\times$ (and $d \mid \zeta\delta$). Hence the number of choices for m is $\varphi(\zeta\delta)/\varphi[\operatorname{lcm}(d,\delta)]$.

Now

$$\varphi[\operatorname{lcm}(d,\delta)] = \varphi\left(\frac{d\delta}{\gcd(d,\delta)}\right) = \frac{\varphi(d)\varphi(\delta)}{\varphi[\gcd(d,\delta)]} = \frac{\varphi(d)\varphi(\delta)}{w}.$$

So the number of choices for m is $\frac{\varphi(\zeta\delta)w}{\varphi(d)\varphi(\delta)}$.

There are $\varphi(\gamma)$ choices for $i \in \mathbb{Z}_\gamma^\times$ and γ choices for $j \in \mathbb{Z}_\gamma$.

Therefore, the number of pairs (x, y) of generators satisfying (5.5) and (5.8) is

$$\begin{aligned} \sharp \text{ of pairs of generators } (x,y) &= \frac{\varphi(\gamma)\gamma\varphi(\zeta\delta)w}{\varphi(d)\varphi(\delta)} \\ &= \frac{\gamma\varphi(n)w}{\varphi(d)\varphi(\delta)} \\ &= \frac{\gamma\varphi(e)w}{\varphi(\delta)}, \end{aligned}$$

in each subgroup. □

Lemma 5.2.2 shows that the regular subgroups of $\mathrm{Hol}(G)$ isomorphic to Γ fall into w disjoint families $F_1, \ldots, F_w$, where F_h consists of those subgroups with a pair of generators (X, Y) satisfying (5.5) and (5.8) for the orbit representatives κ_h of $\mathcal{K}$ under the action of group Δ.

(We will see later that all the F_h are nonempty.) However, not every pair of elements (X, Y) satisfying (5.5) and $YX = X^{\kappa_h}Y$ will generate a regular subgroup. We now characterise those that do.

Lemma 5.2.3. Let $1 \leq h \leq w$ and let $X, Y \in \mathrm{Hol}(G)$ be as in (5.5). Suppose further that X and Y satisfy

$$YX = X^{\kappa_h}Y.$$

Then the subgroup $\langle X, Y\rangle \subseteq \mathrm{Hol}(G)$ is regular on G if and only if

(i) the group $\langle X\rangle$ acts regularly on the subset $\{\sigma^{em/\gamma} : m \in \mathbb{Z}\}$ of G of cardinality γ;

(ii) $Y^{\zeta\delta} = 1$;

(iii) the group $\langle X, Y^d\rangle$ acts transitively on the subset $\{\sigma^m : m \in \mathbb{Z}\}$ of G of cardinality e.

Proof. Suppose X, Y satisfy (i), (ii) and (iii), and let $\Gamma^* = \langle X, Y\rangle$. By (i), X has order γ, and since Y contains τ with exponent 1, for an arbitrary element $\sigma^i\tau^j$ we have $Y^{-j} \cdot \sigma^i\tau^j \in \{\sigma^m : m \in \mathbb{Z}\}$ so it follows from (iii) that Γ^* is transitive on G. Then, from (ii) the order of Y divides $\zeta\delta$. On the other hand, as $Y^j \cdot 1_G = \sigma^{A(j)}\tau^j$ for some $A(j)$ and τ has order d, the order of Y is divisible by d. If Y has order less than $\zeta\delta$, then, using the commutation relation $YX = X^{\kappa_h}Y$, $|\langle X, Y^d\rangle| < \gamma(\zeta\delta/d) = e$ contradicting (iii). It follows that Y has order $\zeta\delta$ and $|\Gamma^*| = |G| = n$. Hence Γ^* is regular.

Conversely, suppose $\Gamma^* = \langle X, Y\rangle$ is regular.

Then (i) follows from Proposition 5.2.1, so in particular X has order γ. Since $|\Gamma^*| = n = \gamma\zeta\delta$, then (ii) follows. Since Y^d does not involve τ, the subgroup $\langle X, Y^d\rangle$ of index d acts on $\{\sigma^m : m \in \mathbb{Z}\}$ and this action must be regular, and hence transitive. Then (iii) holds. □

Definition 5.2.4. Given h with $1 \leqslant h \leqslant w$. Let N_h be the number of quintuples

$$(a, c, u, v, t) \in \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e^\times$$

such that the elements X, $Y \in \mathrm{Hol}(G)$ defined by the form (5.5) generate a regular subgroup isomorphic to Γ and satisfy the relation $YXY^{-1} = X^{\kappa_h}$.

5.3 Calculating N_h

For each prime $q \mid e$, let $r_q = \mathrm{ord}_q(k)$, and for each prime $q \mid \epsilon$, let $\rho_q = \mathrm{ord}_q(\kappa)$. Thus we have

$$r_q = 1 \Leftrightarrow q \mid z;$$

$$r_q \mid \gcd(d, q-1);$$

$$\mathrm{lcm}\{r_q : q \mid e\} = \mathrm{lcm}\{r_q : q \mid g\} = d.$$

Note that the data $(r_q)_{q|e}$ does not in general determine the isomorphism class of G,

and is not in general determined by the factorisation $n = dgz$. Also note that (like g and z) the r_q are isomorphism invariants: they are unchanged if we replace k by k' with $G(d, e, k) \cong G(d, e, k')$.

Define the sets of primes S_h and T as

$$\begin{aligned} S_h &= \{q\colon q \mid \gcd(g, \gamma),\ r_q = \rho_q > 2\colon \kappa_h \equiv k^{\pm 1} \pmod{q}\}. \\ T &= \{q\colon q \mid \gcd(g, \gamma),\ r_q = \rho_q = 2\}. \end{aligned}$$

Note if $\kappa_{h'} = \kappa_h^{-1}$ then $S_{h'} = S_h$, and S_h is independent of the coset representatives κ_h since $r_q \mid \gcd(d, \delta)$.

Now fix a particular h.

For the rest of this section, to simplify the notations, write κ for κ_h.

Let X and Y be as in (5.5). We will translate conditions (i), (ii) and (iii) of Lemma 5.2.3 and (5.8) into congruence conditions on the components of the quintuple (a, c, u, v, t) modulo each prime $q \mid e$. Thus we need to determine a, u, t mod q for all $q \mid e$ and to determine c, v mod q just for $q \mid g$.

Proposition 5.3.1. Condition (i) of Lemma 5.2.3 is equivalent to the following conditions at all primes $q \mid e$:

$$\text{if } q \mid \gamma \text{ then } a \not\equiv 0; \tag{5.9}$$

$$\text{if } q \mid \zeta\delta \text{ then } a \equiv 0; \tag{5.10}$$

$$\text{if } q \mid g \text{ and } q \mid \zeta\delta \text{ then } c \equiv 0. \tag{5.11}$$

Proof. (i) is equivalent to

$$X^\gamma = 1, \qquad X^j \cdot 1_G = 1_G \Leftrightarrow \gamma \mid j.$$

As $X^j = [\sigma^{aj}, \theta^{cj}]$, the second of these is equivalent to

$$e \mid aj \Leftrightarrow \gamma \mid j,$$

and hence to $\gcd(a, e) = e/\gamma$, which is the same as (5.9) and (5.10). (Note that $q \nmid \gamma \Leftrightarrow q \mid \zeta\delta$.) Then $X^\gamma = 1$ when we also have $c\gamma \equiv 0 \pmod{g}$, giving (5.11). □

Proposition 5.3.2. Assume that (5.9), (5.10), (5.11) hold. Then condition (5.8) is equivalent to the following conditions for each prime $q \mid e$:

$$\text{if } q \mid \gamma \text{ and } q \mid z \text{ then } t \equiv \kappa; \tag{5.12}$$

$$\begin{aligned} &\text{if } q \mid \gamma, q \mid g \text{ then} \\ &\quad \text{either} \quad t \equiv \kappa, \quad a(1-k) + zc \equiv 0, \\ &\quad \text{or} \quad\ \ tk \equiv \kappa, \quad c \equiv 0. \end{aligned} \tag{5.13}$$

Proof. Expanding (5.8) gives

$$[\sigma^{u+atk}\tau, \theta^{v+ct}\phi_t] = [\sigma^{a\kappa+u+zc\kappa}\tau, \theta^{c\kappa+v}\phi_t]$$

which is equivalent to

(a) $(\kappa - tk)a + zc\kappa \equiv 0 \pmod{e}$, and

(b) $(t - \kappa)c \equiv 0 \pmod{g}$.

Note that, although κ is only defined mod δ, these make sense because of (5.10) and (5.11). We determine when (a) and (b) hold mod q for each prime q.

When $q \mid \zeta\delta$, (a) and (b) are automatically satisfied because of (5.10), (5.11). So suppose $q \mid \gamma$.

If $q \mid z$ then (b) is irrelevant and (a) reduces to $(\kappa - t)a \equiv 0$ since $k \equiv 1$. By (5.9), this is the same as (5.12).

Now let $q \mid g$. If $t \equiv \kappa$ then (b) holds for any choice of c, and, substituting into (a), we get the first case of (5.13). If $t \not\equiv \kappa$ then (b) gives $c \equiv 0$, and then (a) reduces to $\kappa \equiv tk$, again using (5.9). This gives the second case of (5.13). □

Proposition 5.3.3. Suppose that conditions (i) of Lemma 5.2.3 and (5.8) hold. Then the condition (iii) of Lemma 5.2.3 is equivalent to

$$\text{if } q \mid \zeta\delta \text{ and } q \mid z \text{ then } t \equiv 1 \text{ and } u \not\equiv 0; \tag{5.14}$$

$$\begin{aligned} &\text{if } q \mid \zeta\delta, q \mid g \text{ then} \\ &\quad \text{either} \quad t \equiv 1, \quad v \not\equiv 0, \\ &\quad \text{or} \quad tk \equiv 1, \quad u(1-k) + zvk \not\equiv 0. \end{aligned} \tag{5.15}$$

Moreover, if these hold then the condition (ii) of Lemma 5.2.3 is equivalent to the further conditions

$$\text{if } q \mid \gamma, q \mid g \text{ and } \kappa k \equiv 1, t \equiv \kappa \text{ then } (t-1)u + zv \equiv 0; \tag{5.16}$$

$$\text{if } q \mid \gamma, q \mid g \text{ and } \kappa \equiv k, tk \equiv \kappa \text{ then } v \equiv 0. \tag{5.17}$$

Proof. We have $Y^{di} \cdot 1_G = \sigma^{A(di)}$ with

$$A(di) = uS(tk, di) + zvkT(k, t, di),$$

where $S(s, di)$ and $T(k, s, di)$ are given by (4.2) and (4.3) respectively in Proposition 4.2.2, where s and k are integers such that $s \not\equiv 0 \pmod{q}$ and $k^d \equiv 1 \pmod{q}$, for each prime $q \mid e$ and $i \geq 0$.

Then by (5.6), for any $j \in \mathbb{Z}$ the orbit of σ^j under $\langle X \rangle$ is $\{\sigma^{j+em/\gamma} : m \in \mathbb{Z}\}$. Hence the condition (iii) of Lemma 5.2.3 holds if and only if $A(di)$ represents all residue classes mod e/γ as i varies.

Suppose that (iii) holds. Then by using Proposition 4.2.2, $A(di)$ must represent all residues classes mod q for each prime $q \mid e/\gamma$, that is, for each prime $q \mid e$ with $q \mid \zeta\delta$. First consider primes $q \mid \zeta\delta$ with $q \mid z$. Then $k \equiv 1$ and $A(di) \equiv uS(t, di)$. If $t \not\equiv 1$ then

$$A(di) \equiv \frac{(t^{di} - 1)u}{t - 1}.$$

This cannot represent all residue classes as there is no i with $t^{di} \equiv 0$. So we must have $t \equiv 1$. Note that

$$A(di) \equiv udi \text{ if } q \mid \zeta\delta, q \mid z, t \equiv 1. \tag{5.18}$$

For $A(di)$ to represent all residue classes mod q, we require $u \not\equiv 0$. Thus we have shown that (5.14) holds.

Now consider primes $q \mid \zeta\delta$ with $q \mid g$. If $t \not\equiv 1 \not\equiv tk$, then

$$A(di) \equiv \frac{(t^{di} - 1)u}{tk - 1} + zck\frac{(t^{di} - 1)}{k(t - 1)(tk - 1)}.$$

Again, this cannot represent all residue classes mod q since $t^{di} \not\equiv 0$. So if (iii) holds we must have $t \equiv 1$ or $tk \equiv 1$. If $t \equiv 1$ then

$$A(di) \equiv uS(k, di) + zvk\ \frac{di}{k(k - 1)} \equiv \frac{zvdi}{k - 1} \text{ if } q \mid \zeta\delta, q \mid g, t \equiv 1. \tag{5.19}$$

For this to take all values mod q we need $v \not\equiv 0$. This gives the first case of (5.15). If $tk \equiv 1$, we have

$$A(di) \equiv udi + zvk\ \frac{di}{k(t - 1)} \text{ if } q \mid \zeta\delta, q \mid g, tk \equiv 1. \tag{5.20}$$

This takes all values mod q only when $u(t - 1) + zv \not\equiv 0$, giving the second case of (5.15).

Conversely, if (5.14) and (5.15) hold then it follows from (5.18), (5.19) and (5.20) that $A(di)$ represents all residue classes mod q for all relevant q. Moreover, $A(di) \bmod q$

depends only on $i \pmod q$, so by the Chinese Remainder Theorem, $A(di)$ represents all residue classes mod e/γ. Thus (iii) of Lemma 5.2.3 holds.

For the rest of the proof, we suppose that (5.14) and (5.15) hold. Condition (ii) of Lemma 5.2.3 is equivalent to the following two conditions:

$$A(\zeta\delta) \equiv 0 \pmod q \text{ for all primes } q \mid e; \tag{5.21}$$

$$vS(t, \zeta\delta) \equiv 0 \pmod q \text{ for all primes } q \mid g. \tag{5.22}$$

Now (5.21) holds when $q \mid \zeta\delta$ by (5.18), (5.19) and (5.20), together with (5.14) and (5.15). If also $q \mid g$, then (5.22) holds since if $t \equiv 1$ then $S(t, \zeta\delta) = \zeta\delta \equiv 0$ and if $tk \equiv 1$ then again $S(t, \zeta\delta) = 0$ since $t^{\zeta\delta} \equiv 1$.

It remains to show that (5.21) and (5.22) for primes $q \mid \gamma$ are equivalent to (5.16) and (5.17). If $q \mid z$ then $tk \equiv t \equiv \kappa \not\equiv 1$ by (5.12), so $S(tk, \zeta\delta) = 0$. Thus (5.21) holds. If $q \mid g$ then by (5.13) either $t \equiv \kappa$ or $tk \equiv \kappa$. When $t \not\equiv 1 \not\equiv tk$, we have $S(tk, \zeta\delta) \equiv T(t, k, \zeta\delta) \equiv S(t, \zeta\delta) \equiv 0$, so (5.21) and (5.22) hold with no conditions on u, v.

We have to consider the special cases $t \equiv 1$ and $tk \equiv 1$. If $tk \equiv 1$, we cannot have $tk \equiv \kappa$ as $\kappa \not\equiv 1$. We may have $t \equiv \kappa$; this occurs if $\kappa k \equiv 1$. As $t \not\equiv 1$, (5.22) holds for arbitrary v, and (5.21) becomes

$$u\zeta\delta + zv \, \frac{\zeta\delta}{t-1} \equiv 0,$$

giving (5.16). If $t \equiv 1$, we cannot have $t \equiv \kappa$, but we may have $tk \equiv \kappa$; this occurs if $\kappa \equiv k$. In this case (5.22) is equivalent to $v \equiv 0$, and (5.21) holds for arbitrary u. This gives (5.17). □

The following fact is extracted from the proof.

Proposition 5.3.4. If $q \mid e$ and $q \mid \zeta\delta$ then $A(di) \equiv iA(d) \pmod q$ and $A(d) \not\equiv 0$. Also, if $q \mid e$ and $q \mid \gamma$ then $A(di) \equiv 0 \pmod q$.

We now count the quintuples (a, c, u, v, t) for each prime q. For each prime $q \mid e$, we impose the relevant conditions from (5.9)–(5.17).

(I) $q \mid z$, $q \mid \zeta\delta$. We have $a \equiv 0$, $t \equiv 1$, $u \not\equiv 0$, giving $q-1$ quintuples.

(II) $q \mid z$, $q \mid \gamma$. We have $a \not\equiv 0$, $t \equiv \kappa$, u arbitrary, giving $q(q-1)$ quintuples.

(III) $q \mid g$, $q \mid \zeta\delta$. We have $a \equiv c \equiv 0$, $t \equiv 1$ or $tk \equiv 1$. In either case we have $q(q-1)$ pairs (u, v), giving $2q(q-1)$ quintuples.

(IV) $q \mid g$ and $q \mid \gamma$. We have $a \not\equiv 0$, $t \equiv \kappa$ or $tk \equiv \kappa$ (with c determined by a). Moreover, if either $t \equiv 1$ or $tk \equiv 1$ then we can choose u arbitrarily but once this is done, only one choice of v allowed. This situation can only arise for special values of κ. In general, we have no restrictions on u and v. Thus we need to examine various cases:

(a) Suppose $\kappa \not\equiv k$ and $\kappa \not\equiv k^{-1}$. (This happens if $r_q \neq \rho_q$, or if $r_q = \rho_q > 2$ but $q \notin S_h$.) In this case we have no restrictions on u and v, so we get $2q^2(q-1)$ quintuples.

(b) Suppose $\kappa \equiv k \equiv k^{-1}$ (or, equivalently, that $r_q = \rho_q = 2$.) If $t \equiv \kappa$ then $tk \equiv 1$. If $tk \equiv \kappa$ then $t \equiv 1$. In each case, we may choose u arbitrarily but then v is determined. Thus we have $2(q-1)q$ quintuples.

(c) Suppose $\kappa \equiv k \not\equiv k^{-1}$. (This occurs only if $r_q = \rho_q > 2$ and $q \in S_h$.) If $t \equiv \kappa$ then $t \not\equiv 1 \not\equiv tk$, and we have $q^2(q-1)$ choices for the other parameters. If $tk \equiv \kappa$ then $t \equiv 1$ and we have only $q(q-1)$ choices. This gives $q(q-1)(q+1)$ quintuples.

(d) Suppose $\kappa \equiv k^{-1} \not\equiv k$. (This occurs only if $r_q = \rho_q > 2$ i.e. $q \in S_h$.) If $tk \equiv \kappa$ then $t \not\equiv 1 \not\equiv tk$, and we have $q^2(q-1)$ choices for the other parameters. If $t \equiv \kappa$ then $tk \equiv 1$ and we have only $q(q-1)$ choices. Again, this gives $q(q-1)(q+1)$ quintuples.

The Table 5.1 shows the values and number of quintuples (a, c, u, v, t) for each prime q. In Table 5.1, we consistently use the notations below

$$\begin{aligned}
(*): &\quad u(1-k)+zvk \not\equiv 0, \qquad q-1 \text{ choices for } v \text{ given } u.\\
(**): &\quad a(1-k)+zc \equiv 0, \qquad 1 \text{ choices for } c \text{ given } a.\\
(***): &\quad (t-1)u+zv \equiv 0, \qquad q-1 \text{ choices for } v \text{ given } u.
\end{aligned}$$

Table 5.1: Values and number of quintuples (a, c, u, v, t) for each prime q.

Primes q	t	a	u	c	v	# Quintuples
$q \mid z, q \mid \zeta\delta$	1	0	$\neq 0$			$q-1$
$q \mid z, q \mid \gamma$	κ	$\neq 0$	arb.			$q(q-1)$
$q \mid g, q \mid \zeta\delta$	1	0	arb.	0	$\neq 0$	$q(q-1)$
	k^{-1}	0	arb.	0	$(*)$	$q(q-1)$
$q \mid g, q \mid \gamma$	κ	$\neq 0$	arb.	$(**)$	arb.	$q^2(q-1)$
$\kappa \equiv k, \rho_q > 2$ $(q \in S_h)$	$\kappa k^{-1} = 1$	$\neq 0$	arb.	0	0	$q(q-1)$
$q \mid g, q \mid \gamma$	κ	$\neq 0$	arb.	$(**)$	$(***)$	$q(q-1)$
$\kappa \equiv k^{-1}, \rho_q > 2$ $(q \in S_h)$	κk^{-1}	$\neq 0$	arb.	0	arb.	$q^2(q-1)$
$q \mid g, q \mid \gamma$	κ	$\neq 0$	arb.	$(**)$	$(***)$	$q(q-1)$
$\kappa \equiv k \equiv -1$ $(\neq 1)$	$\kappa k^{-1} = 1$	$\neq 0$	arb.	0	0	$q(q-1)$
$q \mid g, q \mid \gamma$	κ	$\neq 0$	arb.	$(**)$	arb.	$q^2(q-1)$
all others	κk^{-1}	$\neq 0$	arb.	0	arb.	$q^2(q-1)$

We know that $A(di)$ represents all residue classes mod q for $q \mid \zeta\delta, q \mid e$. For these primes, we have $A(di) \equiv mdi \pmod q$, where

$$m \equiv \begin{cases} u & \text{if } q \mid z, q \mid \zeta\delta; \\ \dfrac{zv}{k-1} & \text{if } q \mid g, q \mid \zeta\delta, t \equiv 1 \pmod q; \\ u + \dfrac{zvk}{k(t-1)} & \text{if } q \mid g, q \mid \zeta\delta, tk \equiv 1 \pmod q. \end{cases} \tag{5.23}$$

($m \not\equiv 0$ in all the $(*)$ cases.)

Theorem 5.3.5. The number of quintuples

$$(a, c, u, v, t) \in \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e^\times$$

is

$$N_h = \varphi(e)\gamma g 2^{\omega(g)} \left(\prod_{q\in T} \frac{1}{q}\right)\left(\prod_{q\in S_h} \frac{q+1}{2q}\right).$$

Proof. We multiply the contributions listed above for all primes $q \mid e$. Collecting together the factors $q-1$ gives $\varphi(e)$. For the primes of type (IV), the remaining part of the contribution is

$$\begin{cases} 2q^2 & \text{for type (IV)(a);} \\ 2q^2 \times \frac{1}{q} & \text{for type (IV)(b);} \\ 2q^2 \times \frac{q+1}{2q} & \text{for types (IV)(c)(d).} \end{cases}$$

Thus we have

$$\begin{aligned} N_h &= \varphi(e)\left(\prod_{q\mid \gcd(z,\gamma)} q\right)\left(\prod_{q\mid \gcd(g,\zeta\delta)} 2q\right)\left(\prod_{q\mid \gcd(g,\gamma)} 2q^2\right) \\ &\quad \times \left(\prod_{q\in T} \frac{1}{q}\right)\left(\prod_{q\in S_h} \frac{q+1}{2q}\right) \\ &= \varphi(e)\left(\prod_{q\mid \gamma} q\right)\left(\prod_{q\mid g} 2q\right)\left(\prod_{q\in T} \frac{1}{q}\right)\left(\prod_{q\in S_h} \frac{q+1}{2q}\right) \\ &= \varphi(e)\gamma g 2^{\omega(g)} \left(\prod_{q\in T} \frac{1}{q}\right)\left(\prod_{q\in S_h} \frac{q+1}{2q}\right). \end{aligned}$$

□

5.4 Number of Hopf-Galois structures

Lemma 5.4.1. For each h, the number of regular subgroups of $\mathrm{Hol}(G)$ in the family F_h is given by

$$|F_h| = \frac{\varphi(\delta)}{w} g 2^{\omega(g)} \left(\prod_{q\in T} \frac{1}{q}\right)\left(\prod_{q\in S_h} \frac{q+1}{2q}\right).$$

Proof. This is immediate from Lemma 5.2.2, Definition 5.2.4 of N_h and Theorem 5.3.5. Thus as each regular subgroup of $\mathrm{Hol}(G)$ fall into w families and each family F_h consists

of these regular subgroups, so we have obtained the number of regular subgroups in each family as below

$$|F_h| = \frac{1}{\#\text{ Pairs of generators}}\ N_h = \frac{\varphi(\delta)}{\gamma\varphi(e)w}\ N_h = \frac{\varphi(\delta)}{w} g 2^{\omega(g)} \left(\prod_{q\in T}\frac{1}{q}\right)\left(\prod_{q\in S_h}\frac{q+1}{2q}\right).$$

□

Corollary 5.4.2. The total number of regular subgroups of $\mathrm{Hol}(G)$ in the all disjoint families $F_1, \ldots, F_w$ is given by

$$\sum_{h=1}^{w} |F_h| = \frac{\varphi(\delta)}{w} g 2^{\omega(g)} M,$$

where

$$M = \left(\prod_{q\in T}\frac{1}{q}\right)\sum_{h=1}^{w}\left(\prod_{q\in S_h}\frac{q+1}{2q}\right).$$

Proof. This is immediate from Definition 5.2.4 of N_h, Theorem 5.3.5 and Lemma 5.4.1.

□

Theorem 5.4.3. Let G, Γ be groups of squarefree order n. With the above notation, the number of Hopf−Galois structures of type G on a Galois extension with Galois group Γ is 0 if $\gamma \nmid e$, and otherwise it is

$$\frac{\varphi(d)}{w}\gamma 2^{\omega(g)} M.$$

Proof. This follows from Lemma 1.1.1, Proposition 5.2.1 and Corollary 5.4.2. Thus the number of Hopf−Galois structures is

$$\frac{|\mathrm{Aut}(\Gamma)|}{|\mathrm{Aut}(G)|} \times \sum_{h=1}^{w} |F_h| = \frac{\gamma\varphi(\epsilon)}{g\varphi(e)}\frac{\varphi(\delta)}{w} g 2^{\omega(g)} M = \frac{\varphi(d)}{w}\gamma 2^{\omega(g)} M.$$

□

5.5 Hopf−Galois structures with Γ fixed and G varied

We want to count the number of Hopf−Galois structures with some family groups G rather than one particular G with Γ fixed. This changes the perspective from what we had before when G is fixed and we were looking for subgroups inside the $\mathrm{Hol}(G)$ for particular G.

Now we fix Γ. For any group G with $|G| = |\Gamma| = n$ we know the number of Hopf−Galois structures of type G on extension with group Γ. So, we aggregate those are isomorphism types of G for which the r_q's take given values.

Previously k was fixed. Therefore, we now want to count the number of $k \in \mathbb{Z}_e^\times$, so we basically need to make $\mathrm{ord}_q(k) = r_q \ \forall \ q \mid e$, hence $\mathrm{ord}_e(k) = \mathrm{lcm}(r_q) = d$. If we find all these k's, then different k's might give the same group G up to isomorphism. If k has order d, there will be $\varphi(d)$ generators of the same subgroup. Therefore, there are $\varphi(d)$ such k for each isomorphism type of the group G.

For each $q \mid e$, as $r_q \mid q-1$, then there are $\varphi(r_q)$ choices for k modulo q. We have three cases of r_q's:

1. If $r_q \neq \rho_q$: then q does not occur in M, so we just get $\varphi(r_q)$ choices.
2. If $r_q = \rho_q = 2$: then $\varphi(r_q) = 1$.
3. If $r_q = \rho_q > 2$: then we want to look at

$$\sum_{h=1}^{w} \sum_{\substack{k \in \mathbb{Z}_e^\times \\ \mathrm{ord}_q(k) = r_q \ \forall \ q \mid e}} \left(\prod_{q \in S_h(k)} \frac{q+1}{2q} \right),$$

where

$$S_h(k) = \{q : q \mid \gcd(g, \gamma),\ r_q = \rho_q > 2 : k^{\pm 1} \equiv \kappa_h \pmod{q}\}.$$

This is the same as S_h defined previously, but we now indicate the dependence on k, and allow k to run through the elements of $\mathbb{Z}_e^\times$ with $\mathrm{ord}_q(k) = r_q \ \forall q \in \mathbb{Z}_e^\times$.

For the last main theorem we write the element e as product of prime numbers $e = q_1 \cdots q_s \cdot q_{s+1} \cdots q_{s+y} \cdot q_{s+y+1} \cdots q_t$, where $q_1, \ldots, q_s$ are the primes such that $r_{q_j} = \rho_{q_j} > 2$ for $j = 1, \ldots, s$, $q_{s+1}, \ldots, q_{s+y}$ are the primes with $r_{q_j} = \rho_{q_j} = 2$ (i.e. $q_j \in T$) for $j = s+1, \ldots, s+y$ and $q_{s+y+1}, \ldots, q_t$ are the other primes dividing e. (i.e. $r_{q_j} \neq \rho_{q_j}$ or $q_j \nmid \epsilon$ for $j = s+y+1, \ldots, t$).

Theorem 5.5.1. For a given value of r_q, the number of Hopf−Galois structures with fixed Galois group Γ and all G with given $g, z, d, (r_q)_{q|e}$ is

$$\gamma 2^{\omega(g)} \left(\prod_{j=1}^{s+y} \left[\varphi(r_{q_j}) - 1 + \frac{1}{q_j} \right] \right) \left(\prod_{j=s+y+1}^{t} \varphi(r_{q_j}) \right).$$

Proof. The number of Hopf−Galois structures (depending on the formula of Theorem 5.4.3) for fixed Γ and for all G with given g, z, d, $(r_q)_{q|e}$ with $\gamma \mid e$ (we denote this number by # HGSs) is

$$\frac{1}{\varphi(d)} \sum_{\substack{k \in \mathbb{Z}_e^\times \\ \mathrm{ord}_q(k) = r_q \ \forall \ q|e}} \left(\frac{\varphi(d)}{w} \gamma 2^{\omega(g)} M_k \right),$$

where

$$M_k = \left(\prod_{q \in T} \frac{1}{q} \right) \sum_{h=1}^{w} \left(\prod_{q \in S_h(k)} \frac{q+1}{2q} \right).$$

We have to divide by $\varphi(d)$ in the form above, because what we have been counting is the possibility for k, but we obtain the same group G (up to isomorphism) for $\varphi(d)$ values of k.

So

$$\#\ \mathrm{HGSs} = \frac{1}{w} \gamma 2^{\omega(g)} \mathcal{M}, \tag{5.24}$$

where

$$\mathcal{M} = \sum_{\substack{k\in\mathbb{Z}_e^\times \\ \mathrm{ord}_q(k)=r_q\ \forall\ q|e}} M_k.$$

We write $k = (k_1, \ldots, k_t) \in \mathbb{Z}_e^\times = \mathbb{Z}_{q_1}^\times \times \cdots \times \mathbb{Z}_{q_t}^\times$. So we need $\mathrm{ord}_q(k) = r_q$ for each $q \mid e$. For each q_j there are $\varphi(r_{q_j})$ choices of k_j of order r_{q_j}. Then when we sum over k the contribution for that prime is $\varphi(r_q)$ choices for each q, that means $\varphi(r_{q_j})$ choices for k_j for $j = 1, \ldots, t$.

For $q_{s+1}, \ldots, q_t$ they can never possibly appear in $\prod_{q\in S_h(k)} \frac{q+1}{2q}$ because these primes do not include $r_q = \rho_q > 2$. So we have got $\sum_{k_{s+1},\ldots,k_t} 1$, that means $\prod_{j=s+1}^{t} \varphi(r_{q_j})$. Therefore, for each h we have

$$\sum_{\substack{k\in\mathbb{Z}_e^\times \\ \mathrm{ord}_q(k)=r_q\ \forall\ q|e}} \left(\prod_{q\in S_h(k)} \frac{q+1}{2q}\right) = \left[\sum_{k_1,\ldots,k_s} \left(\prod_{j=1}^{s} I_j^{(h)}(k_j)\right)\right] \left(\prod_{j=s+1}^{t} \varphi(r_{q_j})\right).$$

where

$$I_j^{(h)}(k_j) = \begin{cases} \frac{q_j+1}{2q_j} & \text{if } k^{\pm 1} \equiv \kappa_h \pmod{q_j}; \\ \\ 1 & \text{if } k^{\pm 1} \not\equiv \kappa_h \pmod{q_j}. \end{cases}$$

Now we can write

$$\sum_{k_1,\ldots,k_s} \left(\prod_{j=1}^{s} I_j^{(h)}(k_j)\right) = \prod_{j=1}^{s} \left(\sum_{k_j} I_j^{(h)}(k_j)\right),$$

Fix h. We know that k_j are varying, so of the $\varphi(r_{q_j})$ possibilities for k_j, two of them give $I_j^{(h)}(k_j) \neq 1$, so we have $\varphi(r_{q_j}) - 2$ other elements which just give us 1. That means

$$\begin{aligned} \prod_{j=1}^{s} \left(\sum_{k_j} I_j^{(h)}(k_j)\right) &= \prod_{j=1}^{s} \left[2.\frac{q_j+1}{2q_j} + \varphi(r_{q_j}) - 2\right] \\ &= \prod_{j=1}^{s} \left[\varphi(r_{q_j}) - 1 + \frac{1}{q_j}\right]. \end{aligned}$$

Hence,

$$\mathcal{M} = \left(\prod_{q\in T}\frac{1}{q}\right)\sum_{h=1}^{w}\left(\prod_{j=1}^{s}\left[\varphi(r_{q_j})-1+\frac{1}{q_j}\right]\right)\left(\prod_{j=s+1}^{t}\varphi(r_{q_j})\right).$$

The terms in the sum over h do not depend on h. Also, we can combine the products over T and over $1 \le j \le s$ since if $q \in T$ then $\varphi(r_q) - 1 + \frac{1}{q} = \varphi(2) - 1 + \frac{1}{q} = \frac{1}{q}$. Thus

$$\mathcal{M} = w\left(\prod_{j=1}^{s+y}\left[\varphi(r_{q_j})-1+\frac{1}{q_j}\right]\right)\left(\prod_{j=s+y+1}^{t}\varphi(r_{q_j})\right).$$

Therefore, from (5.24) the number of Hopf−Galois structures with Γ fixed and all G with given $g, z, d, (r_q)_{q|e}$ is

$$\gamma 2^{\omega(g)}\left(\prod_{j=1}^{s+y}\left[\varphi(r_{q_j})-1+\frac{1}{q_j}\right]\right)\left(\prod_{j=s+y+1}^{t}\varphi(r_{q_j})\right).$$

□

5.6 Examples

Throughout this section, L/K is a Galois extension of squarefree degree n. So in this section, we produce some examples on various possibilities for two groups G and Γ to be several kinds of Hopf−Galois structures and apply them on our main result to find the number of Hopf−Galois structures. Then we explain through the two and three primes examples how our results recover several results in [Byo04b], [Chi03], [Koh13], and [Koh16].

In the first example, we verify that the results of this chapter agree with Chapter 4 for Γ cyclic.

5.6.1 Γ Cyclic and G Arbitrary Groups

Let G be an arbitrary group of order a squarefree number n, and let the group Γ be cyclic of the same order. Hence $\delta = 1, \gamma = 1, \zeta = n$. Then use the formula of Theorem

5.4.3 to see what happens for the cyclic groups. So whatever d is, since $\delta = 1$, then $w = \varphi[\gcd(d, \delta)] = 1$. Since there is no primes in γ, this implies that the conditions in M do not hold and $S_1 = \emptyset$. So we get $2^{\omega(g)}\varphi(d)$ Hopf−Galois structures on a Galois extension of cyclic type of degree n. This is same result as obtained in Theorem 4.1.1.

5.6.2 Γ Arbitrary and G Cyclic Groups

Let the group G be cyclic of squarefree order n and let the group Γ be arbitrary of the same order. Hence $d = 1, g = 1, z = n$. Then we look at the formula of Theorem 5.4.3 and notice what happens for the cyclic groups. So whatever δ is, since $d = 1$, then $w = \varphi[\gcd(d, \delta)] = 1$. Since there is no primes in g, this implies that the conditions in $M(k, \kappa)$ do not hold and $S_1 = \emptyset$. Thus a Galois extension with Galois group Γ has γ cyclic Hopf−Galois structures.

5.6.3 Γ Dihedral and G Arbitrary Groups

Let G be an arbitrary group of order $n = 2m$ where m is an odd squarefree number and let the group Γ be dihedral of the same order. Hence $\delta = 2, \gamma = m, \zeta = 1$. Then based on the formula of Theorem 5.4.3 to see what happens related to the dihedral groups. Since all the $\rho_q = 2$ for all $q \mid m$ and can not be bigger than 2, and we do not have any cases when $r_q = \rho_q > 2$. So $\gcd(d, \delta)$ can not be bigger than 2, then $w = \varphi[\gcd(d, \delta)] = 1$ and $S_1 = \emptyset$. Thus we have $\varphi(d)m2^{\omega(g)} \prod_{\substack{q:q|g \\ r_q=2}} \frac{1}{q}$ Hopf−Galois structures. Then after some simplifications there are $\varphi(d)2^{\omega(g)} \prod_{\substack{q:q|g \\ r_q\neq 2}} q$ Hopf−Galois structures on a Galois extension of dihedral type of degree n.

5.6.4 Γ Arbitrary and G Dihedral Groups

Let the group G be dihedral of order $n = 2m$ where m is an odd squarefree number and let the group Γ be arbitrary of the same order. Then $d = 2, g = m, z = 1$. Therefore, depending on the formula of Theorem 5.4.3 we look at what happens for the dihedral groups. Since all the $r_q = 2$ for all $q \mid m$ and cannot be bigger than 2, and we do

not have any cases when $r_q = \rho_q > 2$. So $\gcd(d, \delta)$ cannot be bigger than 2, then $w = \varphi[\gcd(d, \delta)] = 1$ and $S_1 = \emptyset$. Hence we have $\gamma 2^{\omega(m)} \prod_{\substack{q:q|\gamma \\ \rho_q=2}} \frac{1}{q}$ Hopf−Galois structures. Therefore, after we simplify that, the number of Hopf−Galois structures on a Galois extension of degree n is $2^{\omega(m)} \prod_{\substack{q:q|\gamma \\ \rho_q \neq 2}} q$.

Now we have this example as special case of §5.6.3 and §5.6.4.

5.6.5 Γ Dihedral and G Dihedral Groups

Let G and Γ be the dihedral groups of order $n = 2m$ where m is an odd squarefree number. Then $d = \delta = 2, g = \gamma = m, z = \zeta = 1$. We catch the formula of Theorem 5.4.3 and see what happens for the dihedral groups as we know all the parameters. Since all the $r_q = \rho_q = 2$ for all $q \mid m$ and can not be bigger than 2, and we do not have any cases when $r_q = \rho_q > 2$. So $\gcd(d, \delta)$ can not be bigger than 2, then $w = \varphi[\gcd(d, \delta)] = 1$ and $S_1 = \emptyset$. Thus a Galois extension of dihedral type of degree n admits $2^{\omega(m)}$ Hopf−Galois structures. It is clear to see that this number of Hopf−Galois structures agrees with the number that we have in example 5.6.3 when we take G diheral group, and in example 5.6.4 when we take Γ dihedral group.

5.6.6 Two Primes

Let $p > q$ be prime. We suppose $q \mid (p - 1)$ since otherwise the cyclic group C_n is the only group of order n with $d = \delta = 1$, $g = \gamma = 1$, $z = \zeta = pq$. So the other group is metabelian $C_p \rtimes C_q$ with $d = \delta = q, g = \gamma = p, z = \zeta = 1$ where C_q acts nontrivially on C_p.

In the Table 5.2, the first column indicates the numbers of cases of the group types G and Γ, the next two columns show the group type of G and Γ, the 4th to 9th columns explain the factorisations $n = dgz$ and $\delta\gamma\zeta$ for which G and Γ exist, and the number of Hopf−Galois structures of each type is shown in the 10th column and depends on the

formula $\frac{\varphi(d)}{w}\gamma 2^{\omega(g)}M$ of Theorem 5.4.3.

From Table 5.2 in case 1, G and Γ are cyclic groups that covers by §5.6.1 and §5.6.2, so the number of Hopf−Galois structures is one and it is the classical one. Whilst, in case 2 when G is cyclic and Γ is metabelian, that covers by §5.6.2, then there are p Hopf−Galois structures. In case 3 when G is metabelian and Γ is cyclic, that covers by §5.6.1. So the number of Hopf−Galois structures is $2(q-1)$. Whilst, in case 4 when G and Γ are metabelian groups, it could be that $q=2$, in which case both G and Γ will be dihedral; this situation is covered by §5.6.5. So the number of Hopf−Galois structures is 2. If $q>2$ then $w=\varphi[\gcd(d,\delta)]=q-1$ and $r_p=\rho_p=q>2$. Hence

for one h, $\kappa\equiv k \pmod p$ then $S_h=\{p\}$

for some $h'\neq h$, $\kappa\equiv k^{-1} \pmod p$ then $S_{h'}=\{p\}$.

So $S_{h^*}=\emptyset$ for $h^*\neq h,h'$.

Therefore, depending on the formula of Theorem 5.4.3, we have a contribution $\frac{p+1}{2p}$ for each of h and h', and a contribution 1 for the remaining $q-3$ values h^*. Then

$$\begin{aligned}
\#\text{ Hopf−Galois structures} &= \frac{q-1}{q-1}\cdot p\cdot 2\cdot 1\cdot\left[\frac{p+1}{2p}+\frac{p+1}{2p}+q-3\right]\\
&= 2p\cdot\left[2\cdot\left(\frac{p+1}{2p}\right)+(q-3)\right]\\
&= 2p\cdot\left[\frac{p+1}{p}+\frac{p(q-3)}{p}\right]\\
&= 2[p+1+p(q-3)]\\
&= 2[p(q-2)+1].
\end{aligned}$$

Table 5.2: Number of Hopf−Galois structures in Theorem 5.4.3 for $n=pq$.

Case	G	Γ	d	g	z	δ	γ	ζ	# HGSs in Theorem 5.4.3
1	C_n	C_n	1	1	pq	1	1	pq	1
2	C_n	$C_p\rtimes C_q$	1	1	pq	q	p	1	p
3	$C_p\rtimes C_q$	C_n	q	p	1	1	1	pq	$2(q-1)$
4	$C_p\rtimes C_q$	$C_p\rtimes C_q$	q	p	1	q	p	1	$2[p(q-2)+1]$

All these results were obtained in [Byo04b]. We also obtained cases 1 and 3 in §4.4.3.

5.6.7 Three Primes

Let $n = p_1p_2p_3$ where $p_1 < p_2 < p_3$ are primes. In this example, the groups G and Γ take six different cases of group types as the types in §4.4.4 that listed in Table 4.2. Thus we split those cases into Tables 5.3 - 5.8, one for each Galois group Γ. Each table shows the number of Hopf−Galois structures of each type G on a Galois extension with given Galois group Γ. The last Table 5.9 depends on congruence conditions relating to the three primes to find the number of isomorphism classes of groups of order n and the total number of Hopf−Galois structures on all Galois extensions of degree $p_1p_2p_3$.

Also, in each table of Tables 5.3 - 5.8 for ease of reference we put the 1st column to enumerate the cases of the factorisations, the 2nd to 7th columns show the factorisations $n = dgz$ and $n = \delta\gamma\zeta$ for which the groups G and Γ respectively exist, the congruence conditions relating to G and Γ are separately shown in the 8th and 9th columns respectively, the 10th column explains the number of isomorphism types of the groups G, and lastly the number of Hopf−Galois structures of each isomorphism type given by the formula $\frac{\varphi(d)}{w}\gamma 2^{\omega(g)}M$ of Theorem 5.4.3 is explained in the 11th column.

In each of Tables 5.3 - 5.8 the group G varies among the six types and each one of these types corresponds to congruence condition as shown in the 8th column. Whilst the group Γ takes the shapes $C_{p_3p_2p_1}$, $C_{p_3} \times (C_{p_2} \rtimes C_{p_1})$, $C_{p_2} \times (C_{p_3} \rtimes C_{p_1})$, $(C_{p_3} \times C_{p_2}) \rtimes_j C_{p_1}$, $C_{p_1} \times (C_{p_3} \rtimes C_{p_2})$, and $C_{p_3} \rtimes C_{p_2p_1}$ respectively in each table. In Table 5.3, since the group Γ is cyclic type, so there is no congruence condition. While the group Γ under the 9th column in the other tables has $p_2 \equiv 1 \pmod{p_1}$, $p_3 \equiv 1 \pmod{p_1}$, $p_2 \equiv p_3 \equiv 1 \pmod{p_1}$, $p_3 \equiv 1 \pmod{p_2}$, and $p_3 \equiv 1 \pmod{p_1p_2}$ respectively. The number of isomorphism types of the group G in the 10th column in these six tables is 1 in all cases except in the cases $4, 10, 16, 22, 28, 34$ when the prime p_1 acts on both primes p_2 and

p_3, so it is $p_1 - 1$ isomorphism groups. Finally, we show by the formula $\frac{\varphi(d)}{w}\gamma 2^{\omega(g)}M$ of Theorem 5.4.3 in the 11th column in these tables the number of Hopf−Galois structures per group. In addition, the number of Hopf−Galois structures per group in the corresponding cases $1-4$ in Tables 5.3, $7-10$ in Table 5.4, $13-16$ in Table 5.5, and $19-22$ in Table 5.6 agrees with Kohl results [Koh16, Theorem 2.4].

In Table 5.7, where $\Gamma = C_{p_1} \times (C_{p_3} \rtimes C_{p_2})$ we confirm that the number of Hopf−Galois structures in the 11th column in the cases $25-30$ agrees with the Kohl's results [Koh13, Theorem 5.1]. Kohl shows that there are six isomorphism types of groups of order mp where $p = 2q+1$ with q an odd prime and $m = 2q$, and they are C_{mp}, $C_p \times D_q$, $F \times C_2$, $C_q \times D_p$, D_{pq}, and $\mathrm{Hol}(C_p)$. In order to make our groups in Table 5.7 equivalent to those groups in [Koh13, Theorem 5.1] we consider that our groups are of order $p_1p_2p_3$ such that $p_1 = 2, p_2 = q, p_3 = 2q+1$. Then when we use these primes in the cases $25, 26, 29, 27, 28, 30$ respectively with the groups above they recover the Kohl's values relating to the number of Hopf−Galois structures in [Koh13, Theorem 5.1]. For example, if $G = C_q \times D_p = C_{p_2} \times (C_{p_3} \rtimes C_{p_1})$ then $z = p_2$, meaning we are in case 27, and the number of Hopf−Galois structures is $2p_3(p_1 - 1) = 2p$.

We now explain that the number of Hopf−Galois structures in the 11th column in the cases $31-35$ in Table 5.8 recovers Childs results [Chi03]. Childs shows that there are at least five nonisomorphic groups G of order $2qp$ different from $\Gamma = \mathrm{Hol}(Z_p)$ with p an odd prime, and let $2q = p - 1$. Then those nonisomorphic groups are denoted by $Z_p \rtimes Z_q \times Z_2$, $D_q \times Z_p$, $D_p \times Z_q$, Z_{2qp}, and D_{pq}, which, in Kohl's notation, are $F \times C_2$, $C_p \times D_q$, $C_q \times D_p$, C_{mp}, and D_{pq} respectively. In order to confirm that the number of Hopf−Galois structures in the 11th column in the cases $31-35$ agrees with those cases in Childs [Chi03, Theorem 4.1] we assume our groups of order $n = p_1p_2p_3$ as $p_1 = 2, p_2 = q, p_3 = p$. So if we apply these primes in the cases $35, 32, 33, 31, 34$ respectively with the groups above, then all these cases agree with Child's values of

Hopf−Galois structures in [Chi03, Theorem 4.1]. Moreover, it is clear to see that these cases $31, 32, 35, 33, 34, 36$ respectively with the groups C_{mp}, $C_p \times D_q$, $F \times C_2$, $C_q \times D_p$, D_{pq}, and $\mathrm{Hol}(C_p)$ recover Kohl's results regarding to the number of Hopf−Galois structures for $\Gamma = \mathrm{Hol}(C_p)$ in [Koh13, Theorem 5.1].

We show in Table 5.9 in the 1st, 2nd and 3rd columns three combination conditions depending on p_1, p_2, p_3 separately. In the 4th column we explain the cases from Tables 5.3 - 5.8 that agree with the corresponding each appropriate congruence conditions where any groups G and Γ exist.

Table 5.3: Numbers of isomorphism types and Hopf–Galois structures for $\Gamma = C_{p_3p_2p_1}$ of order $n = p_1p_2p_3$.

Case	d	g	z	δ	γ	ζ	Condition on G	Condition on Γ	# groups G	# HGS per group
1	1	1	$p_1p_2p_3$	1	1	$p_1p_2p_3$			1	1
2	p_1	p_2	p_3	1	1	$p_1p_2p_3$	$p_2 \equiv 1 \pmod{p_1}$		1	$2(p_1-1)$
3	p_1	p_3	p_2	1	1	$p_1p_2p_3$	$p_3 \equiv 1 \pmod{p_1}$		1	$2(p_1-1)$
4	p_1	p_2p_3	1	1	1	$p_1p_2p_3$	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$		p_1-1	$4(p_1-1)$
5	p_2	p_3	p_1	1	1	$p_1p_2p_3$	$p_3 \equiv 1 \pmod{p_2}$		1	$2(p_2-1)$
6	p_1p_2	p_3	1	1	1	$p_1p_2p_3$	$p_3 \equiv 1 \pmod{p_1p_2}$		1	$2(p_1-1)(p_2-1)$

Table 5.4: Numbers of isomorphism types and Hopf–Galois structures for $\Gamma = C_{p_3} \times (C_{p_2} \rtimes C_{p_1})$ of order $n = p_1p_2p_3$.

Case	d	g	z	δ	γ	ζ	Condition on G	Condition on Γ	# groups G	# HGS per group
7	1	1	$p_1p_2p_3$	p_1	p_2	p_3		$p_2 \equiv 1 \pmod{p_1}$	1	p_2
8	p_1	p_2	p_3	p_1	p_2	p_3	$p_2 \equiv 1 \pmod{p_1}$	$p_2 \equiv 1 \pmod{p_1}$	1	$2[p_2(p_1-2)+1]$
9	p_1	p_3	p_2	p_1	p_2	p_3	$p_3 \equiv 1 \pmod{p_1}$	$p_2 \equiv 1 \pmod{p_1}$	1	$2p_2(p_1-1)$
10	p_1	p_2p_3	1	p_1	p_2	p_3	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	$p_2 \equiv 1 \pmod{p_1}$	p_1-1	$4[p_2(p_1-2)+1]$
11	p_2	p_3	p_1	p_1	p_2	p_3	$p_3 \equiv 1 \pmod{p_2}$	$p_2 \equiv 1 \pmod{p_1}$	1	$2p_2(p_2-1)$
12	p_1p_2	p_3	1	p_1	p_2	p_3	$p_3 \equiv 1 \pmod{p_1p_2}$	$p_2 \equiv 1 \pmod{p_1}$	1	$2p_2(p_1-1)(p_2-1)$

Table 5.5: Numbers of isomorphism types and Hopf–Galois structures for $\Gamma = C_{p_2} \times (C_{p_3} \rtimes C_{p_1})$ of order $n = p_1p_2p_3$.

Case	d	g	z	δ	γ	ζ	Condition on G	Condition on Γ	# groups G	# HGS per group
13	1	1	$p_1p_2p_3$	p_1	p_3	p_2		$p_3 \equiv 1 \pmod{p_1}$	1	p_3
14	p_1	p_2	p_3	p_1	p_3	p_2	$p_2 \equiv 1 \pmod{p_1}$	$p_3 \equiv 1 \pmod{p_1}$	1	$2p_3(p_1-1)$
15	p_1	p_3	p_2	p_1	p_3	p_2	$p_3 \equiv 1 \pmod{p_1}$	$p_3 \equiv 1 \pmod{p_1}$	1	$2[p_3(p_1-2)+1]$
16	p_1	p_2p_3	1	p_1	p_3	p_2	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	$p_3 \equiv 1 \pmod{p_1}$	p_1-1	$4[p_3(p_1-2)+1]$
17	p_2	p_3	p_1	p_1	p_3	p_2	$p_3 \equiv 1 \pmod{p_2}$	$p_3 \equiv 1 \pmod{p_1}$	1	$2p_3(p_2-1)$
18	p_1p_2	p_3	1	p_1	p_3	p_2	$p_3 \equiv 1 \pmod{p_1p_2}$	$p_3 \equiv 1 \pmod{p_1}$	1	$2p_3(p_1-1)(p_2-1)$

Table 5.6: Numbers of isomorphism types and Hopf–Galois structures for $\Gamma = (C_{p_3} \times C_{p_2}) \rtimes_j C_{p_1}$ of order $n = p_1p_2p_3$.

Case	d	g	z	δ	γ	ζ	Condition on G	Condition on Γ	# groups G	# HGS per group
19	1	1	$p_1p_2p_3$	p_1	p_2p_3	1		$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	1	p_2p_3
20	p_1	p_2	p_3	p_1	p_2p_3	1	$p_2 \equiv 1 \pmod{p_1}$	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	1	$2p_3[p_2(p_1-2)+1]$
21	p_1	p_3	p_2	p_1	p_2p_3	1	$p_3 \equiv 1 \pmod{p_1}$	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	1	$2p_2[p_3(p_1-2)+1]$
22	p_1	p_2p_3	1	p_1	p_2p_3	1	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	p_1-1	$4[p_2(p_1-2)+1][p_3(p_1-2)+1]$
23	p_2	p_3	p_1	p_1	p_2p_3	1	$p_3 \equiv 1 \pmod{p_2}$	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	1	$2p_2p_3(p_2-1)$
24	p_1p_2	p_3	1	p_1	p_2p_3	1	$p_3 \equiv 1 \pmod{p_1p_2}$	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	1	$2p_2p_3(p_1-1)(p_2-1)$

Table 5.7: Numbers of isomorphism types and Hopf–Galois structures for $\Gamma = C_{p_1} \times (C_{p_3} \rtimes C_{p_2})$ of order $n = p_1 p_2 p_3$.

Case	d	g	z	δ	γ	ζ	Condition on G	Condition on Γ	# groups G	# HGS per group
25	1	1	$p_1p_2p_3$	p_2	p_3	p_1		$p_3 \equiv 1 \pmod{p_2}$	1	p_3
26	p_1	p_2	p_3	p_2	p_3	p_1	$p_2 \equiv 1 \pmod{p_1}$	$p_3 \equiv 1 \pmod{p_2}$	1	$2p_3(p_1-1)$
27	p_1	p_3	p_2	p_2	p_3	p_1	$p_3 \equiv 1 \pmod{p_1}$	$p_3 \equiv 1 \pmod{p_2}$	1	$2p_3(p_1-1)$
28	p_1	p_2p_3	1	p_2	p_3	p_1	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	$p_3 \equiv 1 \pmod{p_2}$	p_1-1	$4p_3(p_1-1)$
29	p_2	p_3	p_1	p_2	p_3	p_1	$p_3 \equiv 1 \pmod{p_2}$	$p_3 \equiv 1 \pmod{p_2}$	1	$2[p_3(p_2-2)+1]$
30	p_1p_2	p_3	1	p_2	p_3	p_1	$p_3 \equiv 1 \pmod{p_1p_2}$	$p_3 \equiv 1 \pmod{p_2}$	1	$2p_3(p_1-1)(p_2-1)$

Table 5.8: Numbers of isomorphism types and Hopf–Galois structures for $\Gamma = C_{p_3} \rtimes C_{p_2p_1}$ of order $n = p_1 p_2 p_3$.

Case	d	g	z	δ	γ	ζ	Condition on G	Condition on Γ	# groups G	# HGS per group
31	1	1	$p_1p_2p_3$	p_1p_2	p_3	1		$p_3 \equiv 1 \pmod{p_1p_2}$	1	p_3
32	p_1	p_2	p_3	p_1p_2	p_3	1	$p_2 \equiv 1 \pmod{p_1}$	$p_3 \equiv 1 \pmod{p_1p_2}$	1	$2p_3(p_1-1)$
33	p_1	p_3	p_2	p_1p_2	p_3	1	$p_3 \equiv 1 \pmod{p_1}$	$p_3 \equiv 1 \pmod{p_1p_2}$	1	$2p_3(p_1-1)$
34	p_1	p_2p_3	1	p_1p_2	p_3	1	$p_2 \equiv p_3 \equiv 1 \pmod{p_1}$	$p_3 \equiv 1 \pmod{p_1p_2}$	p_1-1	$4p_3(p_1-1)$
35	p_2	p_3	p_1	p_1p_2	p_3	1	$p_3 \equiv 1 \pmod{p_2}$	$p_3 \equiv 1 \pmod{p_1p_2}$	1	$2p_3(p_2-1)$
36	p_1p_2	p_3	1	p_1p_2	p_3	1	$p_3 \equiv 1 \pmod{p_1p_2}$	$p_3 \equiv 1 \pmod{p_1p_2}$	1	$2[p_3(p_1p_2-p_1-p_2)+1]$

Table 5.9: The cases which occur for different combinations of congruence conditions.

$p_2 \mid (p_3 - 1)$	$p_1 \mid (p_3 - 1)$	$p_1 \mid (p_2 - 1)$	Cases
no	no	no	1
no	no	yes	1, 2, 7, 8
no	yes	no	1, 3, 13, 15
no	yes	yes	1, 2, 3, 4, 7, 8, 9, 10, 13, 14, 15, 16, 19, 20, 21, 22
yes	no	no	1, 5, 25, 29
yes	no	yes	1, 2, 5, 7, 8, 11, 25, 26, 29
yes	yes	no	1, 3, 5, 6, 13, 15, 17, 18, 25, 27, 29, 30, 31, 33, 35, 36
yes	yes	yes	$1, \ldots, 36$

Bibliography

[AB18] Ali A. Alabdali and Nigel P. Byott. Counting Hopf−Galois structures on cyclic field extensions of squarefree degree. *J. Algebra*, 493:1–19, 2018.

[BC12] Nigel P. Byott and Lindsay N. Childs. Fixed−point free pairs of homomorphisms and nonabelian Hopf−Galois structures. *New York J. Math.*, 18:707–731, 2012.

[Byo96] Nigel P. Byott. Uniqueness of Hopf−Galois structure for separable field extensions. *Comm. Algebra*, 24(10):3217–3228, 1996.

[Byo04a] Nigel P. Byott. Hopf−Galois structures on field extensions with simple Galois groups. *Bull. London Math. Soc.*, 36(1):23–29, 2004.

[Byo04b] Nigel P. Byott. Hopf−Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra*, 188(1-3):45–57, 2004.

[Byo13] Nigel P. Byott. Nilpotent and abelian Hopf−Galois structures on field extensions. *J. Algebra*, 381:131–139, 2013.

[Byo15] Nigel P. Byott. Solubility criteria for Hopf−Galois structures. *New York J. Math.*, 21:883–903, 2015.

[CC99] Scott Carnahan and Lindsay Childs. Counting Hopf−Galois structures on non−abelian Galois field extensions. *Journal of Algebra*, 218(1):81–92, 1999.

[CC07] Lindsay N. Childs and Jesse Corradino. Cayley's theorem and Hopf−Galois

structures for semidirect products of cyclic groups. *Journal of Algebra*, 308(1):236–251, 2007.

[Chi89] Lindsay N. Childs. On the Hopf−Galois theory for separable field extensions. *Comm. Algebra*, 17(4):809–825, 1989.

[Chi00] Lindsay N. Childs. *Taming wild extensions: Hopf algebras and local Galois module theory*, volume 80 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2000.

[Chi03] Lindsay N. Childs. On Hopf−Galois structures and complete groups. *New York J. Math.*, 9:99–115, 2003.

[Chi05] Lindsay N. Childs. Elementary abelian Hopf−Galois structures and polynomial formal groups. *J. Algebra*, 283(1):292–316, 2005.

[CRV16] Teresa Crespo, Anna Rio, and Montserrat Vela. Induced Hopf−Galois structures. *J. Algebra*, 457:312–322, 2016.

[CS69] Stephen U. Chase and Moss E. Sweedler. Hopf algebras and Galois theory. In *Hopf Algebras and Galois Theory*, volume 97, pages 52–83. Springer–Verlag, Berlin–New York, 1969.

[Dri92] Vladimir G. Drinfeld. On some unsolved problems in quantum group theory. In *Quantum groups*, volume 1510 of *Lecture Notes in Mathematics*, pages 1–8. Springer, Berlin, 1992.

[GP87] Cornelius Greither and Bodo Pareigis. Hopf−Galois theory for separable field extensions. *J. Algebra*, 106(1):239–258, 1987.

[GV17] Leandro Guarnieri and Leandro Vendramin. Skew braces and the Yang−Baxter equation. *Mathematics of Computation*, 86(307):2519–2534, 2017.

[Höl95] Otto Hölder. Die Gruppen mit quatratfreier Ordnungszahl. *Nachr. Königl. Ges. Wiss. Göttingen Math. Phys.*, 1:211–229, 1895.

[Koh98] Timothy Kohl. Classification of the Hopf−Galois structures on prime power radical extensions. *J. Algebra*, 207(2):525–546, 1998.

[Koh13] Timothy Kohl. Regular permutation groups of order mp and Hopf−Galois structures. *Algebra Number Theory*, 7(9):2203–2240, 2013.

[Koh16] Timothy Kohl. Hopf−Galois structures arising from groups with unique subgroup of order p. *Algebra Number Theory*, 10(1):37–59, 2016.

[MM84] M. Ram Murty and V. Kumar Murty. On groups of squarefree order. *Math. Ann.*, 267(3):299–309, 1984.

[Rob96] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer–Verlag, New York, second edition, 1996.